

[PayPal](#)

>> [Lihat semua perjanjian undang-undang](#)

Pengawal kepada Pengawal SCC



[Cetak](#)



[Muat turun PDF](#)

Kemas kini terakhir: 8 Jun 2022

Fasal Kontraktual Standard Pengawal ke Pengawal ("SCC") ini membentuk sebahagian daripada Perjanjian Pengguna PayPal ("Perjanjian") yang terpakai di antara anda, yang bertindak sebagai penjual ("anda" atau "Peniaga") dengan PayPal dan digabungkan oleh rujukan di dalamnya. Sekiranya terdapat apa-apa percanggahan di antara terma SCC ini dengan Perjanjian, terma SCC ini akan mengawal. Terma berhuruf besar yang digunakan tetapi tidak ditakrifkan dalam SCC ini hendaklah mempunyai maksud yang dinyatakan dalam Perjanjian.

Setakat yang terpakai: (i) tindakan anda menandatangani Perjanjian akan dianggap sebagai tandatangan dan penerimaan Keputusan Pelaksanaan Suruhanjaya Eropah (EU) 2021/914 bertarikh 4 Jun 2021 berkenaan fasal kontrak standard untuk pemindahan data peribadi ke negara ketiga selaras dengan Peraturan (EU) 2016/679 ("Fasal Pindahan EU") oleh Peniaga, sebagai pengeksport data dan berperanan sebagai pengawal; (ii) tandatangan PayPal terhadap Perjanjian akan dianggap sebagai tandatangan dan penerimaan Fasal Pindahan EU oleh PayPal, sebagai pengimport data dan berperanan sebagai pengawal; dan (iii) pihak-pihak ini akan tertakluk pada peruntukan Modul 1 Fasal Pindahan EU.

Sekiranya Suruhanjaya Eropah menyemak semula dan selepas itu menerbitkan Fasal Pindahan EU yang baharu (atau seperti yang dikehendaki atau dilaksanakan oleh Suruhanjaya Eropah), pihak-pihak ini bersetuju bahawa Fasal Pindahan EU yang baharu itu akan menggantikan Fasal Pindahan EU yang sedia ada dan mereka akan mengambil semua tindakan sedemikian yang diperlukan untuk melaksanakan pelaksanaan Fasal Pindahan EU yang baharu.

Fasal Pindahan EU (Modul 1) akan digabungkan ke dalam Perjanjian sebagai rujukan dan akan dianggap disempurnakan dengan sewajarnya di antara pihak-pihak ini apabila Perjanjian ini berkuat kuasa tertakluk pada butiran berikut:

- i. pilihan 1 Fasal 17 (Undang-undang yang mentadbir) akan terpakai dan undang-undang Luxembourg akan mentadbir Fasal Pindahan EU;

- i. selaras dengan Fasal 18 (Pilihan forum dan bidang kuasa), mahkamah Luxembourg akan menyelesaikan apa-apa pertikaian yang timbul daripada Fasal Pindahan EU; dan
- ii. pihak-pihak ini bersetuju bahawa butiran yang diperlukan di bawah Lampiran Fasal Pindahan EU adalah seperti yang dinyatakan pada Lampiran 1.

Lampiran 1

Lampiran untuk Fasal Pindahan EU

Lampiran 1.A. Perkara yang berikut terpakai, setakat yang diperlukan, di bawah Fasal Pindahan EU

Pengeksport Data

- Nama dan Alamat: Pengeksport data ialah Peniaga dan alamat adalah seperti yang dinyatakan dalam Perjanjian
- Nama, jawatan dan butiran hubungan orang hubungan: seperti yang dinyatakan dalam Perjanjian
- Aktiviti yang berkaitan dengan data yang dipindahkan di bawah Fasal Kontrak Standard: seperti yang dinyatakan dalam Perjanjian
- Tandatangan dan tarikh: sila rujuk perkara yang disediakan dalam SCC ini
- Peranan (pengawal/pemproses): pengawal

Pengimport Data

- Nama dan Alamat: Pengimport data ialah ahli Kumpulan PayPal yang menyediakan perkhidmatan menurut Perjanjian dan alamat adalah seperti yang dinyatakan dalam Perjanjian
- Nama, jawatan dan butiran hubungan orang hubungan: seperti yang dinyatakan dalam Perjanjian
- Aktiviti yang berkaitan dengan data yang dipindahkan di bawah Fasal Kontrak Standard: seperti yang dinyatakan dalam Perjanjian
- Tandatangan dan tarikh: sila rujuk perkara yang disediakan dalam SCC ini
- Peranan (pengawal/pemproses): pengawal

Lampiran 1.B. Perihal Pindahan

Subjek data yang Data Peribadinya Dipindahkan

Data peribadi yang dipindahkan melibatkan kategori subjek data yang berikut:

- Pelanggan, pekerja dan kenalan perniagaan lain pengeksport data.

Kategori Data Peribadi yang Dipindahkan

- Nama, amaun yang akan dikenakan, tarikh/masa, butiran akaun bank, butiran kad bayaran, kod CVC, poskod, kod negara, alamat, alamat e-mel, faks, telefon, laman web, data tamat tempoh, butiran pengiriman, status cukai, pengenalan pasti pelanggan unik, Alamat IP, lokasi dan apa-apa data lain yang diterima oleh PayPal di bawah Perjanjian.

Data sensitif (jika sesuai) dan Sekatan atau Perlindungan yang Digunakan

Data peribadi yang dipindahkan melibatkan kategori data sensitif yang berikut:

- Tidak berkenaan, kecuali Peniaga mengkonfigurasi perkhidmatan untuk mengambil data tersebut.

Mengenakan sekat dan perlindungan:

- Tidak berkenaan, kecuali Peniaga mengkonfigurasi perkhidmatan untuk mengambil data tersebut.

Sifat Pemprosesan

Seperti yang dinyatakan dalam Perjanjian.

Tujuan Pindahan

Pindahan dibuat untuk tujuan yang berikut:

- Prestasi perkhidmatan yang disediakan oleh pengimport data kepada pengeksport data mengikut Perjanjian.
- Untuk mengenal pasti aktiviti dan risiko penipuan yang, atau mungkin, memberi kesan kepada pengimport data, pengeksport data atau pelanggan lain pengimport data.
- Untuk mematuhi undang-undang dan permintaan penguatkuasaan undang-undang yang terpakai kepada pengimport data.
- Seperti yang dinyatakan dalam Pernyataan Privasi pengimport data.

Tempoh Data Peribadi akan Dikekalkan, atau, jika tidak Mungkin, Kriteria yang Digunakan untuk Menentukan Tempoh tersebut

Pengimport data hanya mengekalkan data peribadi selama yang diperlukan berhubung dengan tujuan relevan data tersebut dikumpulkan (sila lihat tujuan di atas). Untuk

menentukan tempoh pengekalan yang sesuai untuk data peribadi, pengimport data mempertimbangkan amaun, sifat dan kepekaan data peribadi, potensi risiko bahaya daripada penggunaan atau pendedahan data peribadi yang tidak dibenarkan, tujuan data peribadi diproses dan sama ada tujuan tersebut boleh dicapai melalui cara lain, dan keperluan perundangan, kawal selia, cukai, perakaunan atau keperluan lain yang terpakai.

Untuk pindahan kepada (Sub-) Pemproses, juga Nyatakan Perkara Subjek, Sifat dan Tempoh Pemprosesan

Pengimport data boleh berkongsi data peribadi dengan pembekal perkhidmatan pihak ketiga yang melaksanakan perkhidmatan dan fungsi atas arahan pengimport data dan bagi pihaknya. Pembekal perkhidmatan pihak ketiga ini boleh, sebagai contoh, menyediakan elemen perkhidmatan yang disediakan di bawah Perjanjian seperti pengesahan pelanggan, pemprosesan transaksi atau sokongan pelanggan, atau menyediakan perkhidmatan kepada pengimport data yang menyokong perkhidmatan yang disediakan di bawah perjanjian seperti simpanan. Apabila menentukan tempoh pemprosesan yang diambil oleh pembekal perkhidmatan pihak ketiga, pengimport data menggunakan kriteria yang disediakan di atas dalam Lampiran 1.B ini.

Lampiran 1.C. Pihak Berkuasa Penyeliaan

Selaras dengan Fasal 13(a) Fasal Pindahan EU, pihak berkuasa penyeliaan yang bertanggungjawab untuk memastikan pematuan oleh pengeksport data terhadap Peraturan (EU) 2016/679 berkenaan dengan pemindahan data, seperti yang dinyatakan dalam SCC ini, akan bertindak sebagai pihak berkuasa penyeliaan yang kompeten.

B. Langkah-langkah Teknikal dan Organisasi Termasuk Langkah-langkah Teknikal dan Organisasi untuk Memastikan Keselamatan Data

1. Nama samaran, Penyulitan dan Perlindungan Data Semasa Penghantaran.

Polisi PayPal memastikan pematuan kepada prinsip ini dan memerlukan penggunaan kawalan teknikal untuk mengelakkan risiko pendedahan data peribadi. PayPal menggunakan penyulitan dalam transit dan pada masa rehat untuk semua data peribadi. Kami juga menggunakan teknik pemberian nama samaran standard industri, seperti pentokenan untuk melindungi data peribadi jika terpakai. PayPal mempunyai polisi komprehensif yang menyediakan obligasi dan proses utama untuk melindungi data apabila data dipindahkan dalam perusahaan dan secara luaran dengan pihak ketiga.

2. Perubahan Pengurusan dan Kesenambungan Perniagaan.

Proses pengurusan perubahan PayPal yang mantap melindungi ketersediaan dan ketahanan berterusan data dan sistem sepanjang kitaran hayat data dengan memastikan perubahan dirancang, diluluskan, dilaksanakan dan disemak dengan sewajarnya. Proses

pengurusan kesinambungan perniagaan Syarikat menyediakan rangka kerja untuk membina kebingkasan organisasi dengan keupayaan respons yang berkesan yang melindungi kepentingan pihak berkepentingan utamanya.

3. Pemulihan Bencana.

Program bencana mantap PayPal mempunyai proses untuk memulihkan maklumat atau sistem teknologi jika berlaku apa-apa gangguan yang ketara, dengan memberi fokus kepada sistem IT yang menyokong proses perniagaan kritikal dan aktiviti pelanggan. Infrastruktur teknologi PayPal ditempatkan di beberapa pusat data yang selamat, dengan keupayaan utama dan sekunder, masing-masing dilengkapi dengan infrastruktur rangkaian dan keselamatan, aplikasi dan pelayan pangkalan data khusus dan penyimpanan.

4. Ujian Berkala, Penilaian dan Menilai Keberkesanan langkah-langkah Teknikal dan Organisasi.

PayPal sentiasa merancang, melaksanakan dan melaporkan keputusan program ujian Syarikat untuk menaksirkan dan menilai keberkesanan langkah teknologi dan organisasi. Program ini diuruskan menerusi pasukan risiko dan pematuhan perusahaan kami yang bekerjasama dengan pemegang saham yang berkaitan untuk mendapatkan dan menilai maklumat yang diperlukan untuk ujian, pelaporan dan pemulihan jika perlu.

5. Pengenalan dan Pengesahan Pengguna.

Proses pengurusan akses PayPal memerlukan pengguna untuk log masuk ke dalam rangkaian korporat menggunakan ID dan kata laluan akaun rangkaian korporat yang unik untuk pengenalan dan pengesahan pengguna sebelum mengakses apa-apa aplikasi dalam skop lain. Polisi automatik mengenai komposisi, panjang, perubahan, penggunaan semula dan halang masuk kata laluan digunakan. Akses dan kelulusan berdasarkan peranan, yang disahkan setiap suku tahun, dilaksanakan di semua sistem dalam skop untuk menguatkuasakan prinsip yang paling kurang istimewa.

6. Keselamatan Fizikal Lokasi Tempat Data Peribadi Diproses.

Polisi keselamatan global PayPal dan polisi dan proses keselamatan menetapkan keperluan yang diperlukan untuk memudahkan proses keselamatan dan keselamatan, termasuk keselamatan fizikal, mengikut undang-undang, peraturan dan keperluan rakan kongsi yang terpakai. Penekanan khas diberikan kepada sistem keselamatan dan perlindungan apabila membina kawasan khas atau sensitif seperti bilik mel, tempat penyimpanan peralatan, kawasan pengiriman dan penerimaan, bilik komputer/pelayan, peti besi komunikasi atau kawasan penyimpanan dokumen/maklumat sulit, selaras dengan standard pengendalian keselamatan maklumat Syarikat.

7. Pengelogan dan Konfigurasi Peristiwa.

PayPal telah menggariskan dan menentukan jenis dan atribut pengelogan dan pemantauan peristiwa. Syarikat mengumpul dan mengagregatkan beberapa jenis log ke sistem pemantauan keselamatan terpusat. Kawalan pengurusan konfigurasi standard disediakan untuk memastikan log dikumpulkan daripada sistem dan kemudian dikemukakan ke sistem pemantauan keselamatan terpusat kami. Dasar dan proses sokongan PayPal menetapkan bahawa konfigurasi sistem dan garis dasar pengukuhan perlu dilaksanakan di semua sistem.

8. Tadbir Urus dan Pengurusan IT; Pensijilan dan Jaminan Proses dan Produk.

PayPal menggalakkan falsafah keselamatan yang kukuh di seluruh Syarikat. Ketua Pegawai Keselamatan Maklumat kami mengawasi keselamatan maklumat di seluruh perusahaan global kami. Sebagai sebahagian daripada Program Pengurusan Risiko dan Pematuhan Perusahaan kami, Program Pemerhatian Teknologi dan Keselamatan Maklumat kami direka untuk menyokong Syarikat dalam menguruskan risiko keselamatan teknologi dan maklumat dan mengenal pasti, melindungi, mengesan, memberi respons kepada dan memulihkan daripada ancaman keselamatan maklumat. PayPal memperakui dan memastikan proses dan produknya melalui pelbagai program perusahaan, termasuk (i) audit dan penilaian kewajipan standard industri teknikal PayPal termasuk tetapi tidak terhad kepada, ISO 27001, standard Industri Kad Bayaran (PCI) yang terpakai (DSS, PIN, P2PE, dll.) dan Institut Akauntan Awam Bertauliah Amerika (AICPA) SOC-1 dan SOC-2, (ii) Proses Pengenalan Kawalan Risiko (RCIP) yang memastikan penglibatan awal dan pendekatan standard untuk pengukuran, pengurusan dan pemantauan risiko yang berkaitan dengan pembangunan dan pengeluaran penyelesaian produk, (iii) penilaian impak privasi yang disepadukan ke peringkat awal proses pembangunan produk dan perisian, dan (iv) program pengurusan pihak ketiga yang komprehensif, yang memberikan jaminan melalui pengurusan risiko yang berterusan sepanjang kitaran hayat penglibatan dengan pihak ketiga.

9. Peminimuman Data.

Polisi kami memerlukan, melalui kawalan teknikal, elemen data yang dikumpul dan dijana mencukupi, relevan dan terhad kepada perkara yang perlu berkaitan dengan tujuan data diproses. Proses penilaian impak privasi PayPal memastikan pematuhan dengan polisi ini.

10. Kualiti dan Pengekalan Data.

Akses dan polisi kualiti PayPal memastikan bahawa semua data peribadi adalah betul, lengkap dan terkini, yang membolehkan pengguna individu mengakses sistem untuk membetulkan dan mengubah suai butiran mereka (contohnya, alamat, butiran hubungan dll.), dan, jika ada permintaan untuk pembetulan diterima daripada subjek data, untuk menyediakan perkhidmatan yang memberikan hak mereka untuk membuat pembetulan. Program tadbir urus data kami memantau kualiti data, isu dan pemulihan, jika perlu. Kami memerlukan semua data dikelaskan mengikut nilai perniagaannya dengan tempoh pengekalan yang ditetapkan, berdasarkan kepada keperluan perundangan, kawal selia dan

penyimpanan rekod perniagaan PayPal. Setelah tempoh pengekalan tamat, data dan maklumat akan dilupuskan, dipadam atau dimusnahkan.

11. Kebertanggungjawapan

PayPal telah membangunkan satu set polisi dan prinsip keselamatan maklumat, teknologi, tadbir urus data, pengurusan dan privasi pihak ketiga yang selaras dengan standard industri dan direka bentuk untuk melibatkan kerjasama dan perkongsian pemegang saham dalam kesedaran dan pematuhan polisi dan kawalan tersebut di seluruh organisasi untuk memastikan penyertaan dan kebertanggungjawapan merentasi semua peringkat dalam organisasi. Setiap program mentakrifkan kebertanggungjawapan untuk keputusan, proses dan kawalan berkaitan data pelbagai fungsi. Sebagai pengawal data, PayPal bertanggungjawab dan menunjukkan pematuhan terhadap artikel berkaitan yang membawa obligasi kebertanggungjawapan dalam GDPR dan undang-undang perlindungan data lain yang terpakai melalui pelaksanaan polisi program privasi dan struktur kawalan organisasi dan teknikal yang bertingkat untuk memastikan pematuhan perusahaan yang luas ke atas undang-undang, peraturan, polisi dan prosedur privasi. Ini termasuklah kemampuan menunjukkan kepatuhan terhadap undang-undang perlindungan data melalui: 1) budaya pematuhan yang kukuh, 2) struktur tadbir urus risiko dan pematuhan perusahaan yang merangkumi jawatankuasa pengurusan, peranan pemerhatian, pelaporan privasi, 3) kebertanggungjawapan fungsi perniagaan untuk pematuhan program privasi termasuk penubuhan, dokumentasi dan penyelenggaraan proses dan kawalan perniagaan, 4) jabatan privasi global dalam Organisasi Pematuhan Perusahaan untuk mengawasi pematuhan perniagaan dengan program privasi dan menentukan polisi, standard, prosedur dan peralatan yang dikendalikan oleh fungsi perniagaan, 5) komunikasi kepada perusahaan oleh fungsi privasi global untuk menggalakkan kesedaran dan pemahaman tentang privasi, 6) Rangka Kerja Pengurusan Risiko dan Pematuhan Perusahaan untuk memastikan penggunaan proses yang konsisten termasuk penilaian impak privasi, pemantauan dan pengujian privasi, pengurusan isu privasi, latihan privasi, pelan privasi tahunan, dan 7) pelaporan dan analisis kepada jawatankuasa pengurusan yang mengawasi Program Privasi.

12. Hak Subjek Data.

PayPal mempunyai program untuk memastikan hak subjek data dipenuhi, termasuk akses, pembetulan dan pemadaman. Permintaan pemadaman data dipenuhi melainkan PayPal mempunyai sebab perundangan, obligasi kawal selia atau sebab perniagaan lain yang sah untuk mengekalkannya. Polisi PayPal memastikan bahawa pemadaman berlaku sepanjang kitaran hayat pelanggan.

13. Pemproses.

PayPal mempunyai program pengurusan pihak ketiga yang komprehensif, yang memberikan jaminan melalui pengurusan risiko yang berterusan sepanjang kitaran hayat penglibatan dengan pihak ketiga. Kami mempunyai kawalan kontrak yang menghendaki pemproses kami dan subpemproses mereka menyediakan standard keselamatan dan

privasi data yang komprehensif di seluruh rantai pemrosesan. Semua subpemroses perlu mendapatkan kelulusan awal kami sebelum melibatkan diri.