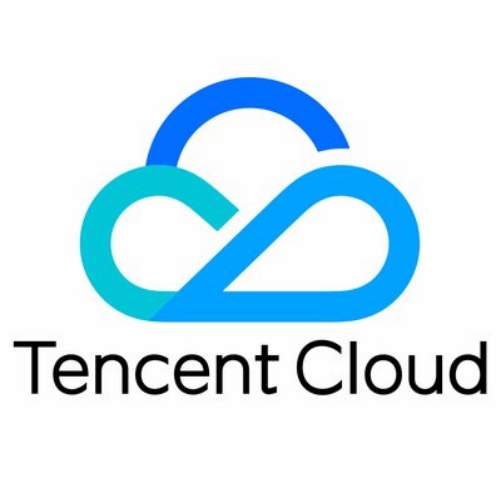
Terms and Policies

Perjanjian Privasi dan Keamanan Data

Dokumen produk



[Pernyataan Hak Cipta]

[Pernyataan Merek Dagang]

Tencent Cloud

dan merek dagang lain yang terkait dengan layanan Tencent Cloud dimiliki oleh perusahaan terkait di bawah Tencent Group. Selain itu, merek dagang pihak ketiga yang disebut dalam dokumen ini merupakan hak milik pemegang haknya sesuai hukum.

[Pernyataan Layanan]

Dokumen ini dimaksudkan untuk memberikan gambaran umum kepada pelanggan tentang seluruh atau sebagian produk dan layanan Tencent Cloud yang terkait pada saat publikasi. Spesifikasi beberapa produk dan layanan dapat disesuaikan. Jenis dan standar layanan atas produk dan layanan Tencent Cloud yang Anda beli akan ditentukan oleh kontrak komersial antara Anda dan Tencent Cloud. Kecuali disepakati lain oleh kedua belah pihak, Tencent Cloud tidak memberikan jaminan tersurat maupun tersirat apa pun terkait isi dokumen ini.

Perjanjian Privasi dan Keamanan Data

Waktu update terbaru：2025-10-11 17:37:42

Sejauh ada konflik antara Adendum Privasi dan Keamanan Data ini (“**DPSA**”) dan Ketentuan Layanan (dan dokumen atau kebijakan apa pun yang digabungkan dengan referensi di dalamnya, kecuali untuk DPSA) (“**Perjanjian**”), DPSA ini adalah yang berlaku.

Definisi

Kecuali dinyatakan sebaliknya istilah-istilah berikut akan memiliki arti yang dianggap berasal dari yang dijelaskan di bawah ini. Istilah dikapitalisasi yang digunakan dalam DPSA ini tetapi tidak didefinisikan di bawah ini akan memiliki makna yang dianggap berasal darinya dalam Perjanjian.
“**Informasi Administratif**” mengacu pada informasi pribadi yang diberikan Organisasi kepada Tencent Cloud untuk mengatur dan mengelola akun Organisasi dan layanan yang disediakan oleh Tencent Cloud, dan informasi pribadi apa pun yang dihasilkan sehubungan dengan penggunaan layanan yang disediakan oleh Tencent Cloud oleh Tencent Cloud;
“**Konten**” mengacu pada data apa pun, termasuk informasi pribadi, yang dikirimkan, diunggah, dikirim, atau ditampilkan oleh Organisasi menggunakan layanan yang disediakan oleh Tencent Cloud;
“**Pengontrol**” mengacu pada seseorang yang baik sendiri atau bersama-sama dengan satu atau lebih orang lain mengontrol pengumpulan, penyimpanan, pemrosesan atau penggunaan Data Pribadi, termasuk sebagaimana berlaku setiap “bisnis” sebagaimana istilah tersebut didefinisikan oleh CCPA;
“**Klausul Transfer Pengontrol-Pemroses**” mengacu pada Klausul Kontrak Standar (Pengontrol ke Pemroses) sebagaimana diatur dalam Keputusan Komisi 5 Februari 2010 (C (2010) 593), sebagaimana ditetapkan di bawah ini pada **(2) Klausul Transfer Pengontrol-Pemroses**;
“**Pelanggaran Data**” mengacu pada penyalahgunaan, gangguan dengan, kehilangan, akses tidak sah ke, modifikasi, atau pengungkapan Data Pribadi yang Diproses oleh Tencent sehubungan dengan Perjanjian;
“**Undang-Undang Perlindungan Data**” mengacu pada undang-undang perlindungan data yang berlaku sehubungan dengan pengumpulan, penyimpanan, pemrosesan, transfer, pengungkapan, dan penggunaan Data Pribadi apa pun yang berlaku dari waktu ke waktu kepada orang atau aktivitas dalam keadaan yang bersangkutan, termasuk Undang-Undang Privasi A.S., Arahan, Arahan e-Privasi, dan GDPR;
“**Subjek Data**” berarti (1) “Subjek Data” sebagaimana istilah tersebut didefinisikan dalam GDPR; (2) “Konsumen” sebagaimana istilah didefinisikan dalam CCPA; atau (3) individu lain yang menjadi subjek Data Pribadi;
“**Arahan**” Mengacu pada Arahan 95/46/EC dari Parlemen Eropa dan Dewan 24 Oktober 1995 tentang perlindungan individu sehubungan dengan Pemrosesan Data Pribadi dan pergerakan bebas data tersebut;
Arahan e-Privasi” mengacu pada Arahan 2002/58/EC dari Parlemen Eropa dan Dewan 12 Juli 2002 tentang Pengolahan Data Pribadi dan perlindungan privasi di sektor komunikasi elektronik;“**EEA**” mengacu pada Wilayah Ekonomi Eropa;
“**Data Pribadi UE**” mengacu pada Data Pribadi subjek data yang berlokasi di EEA;

"**GDPR**" mengacu pada Peraturan 2016/679 dari Parlemen Eropa dan Dewan 27 April 2016 tentang perlindungan orang sehubungan dengan Pemrosesan Data Pribadi dan pergerakan bebas data tersebut;
"**Persyaratan Khusus Yurisdiksi**" mengacu pada persyaratan khusus untuk Memproses Data Pribadi yang berlaku di yurisdiksi tertentu, sebagaimana ditetapkan di bawah ini di **(1) Persyaratan Khusus Yurisdiksi**;
"**Organisasi**" mengacu pada entitas yang telah menyetujui Ketentuan Layanan. Untuk tujuan DPSA ini (termasuk lampirannya), referensi ke "Organisasi" harus, dalam hal perjanjian dengan individu yang tidak bertindak atas nama Organisasi, dianggap sebagai referensi untuk individu tersebut;
"**Data Pribadi**" mengacu pada informasi apa pun yang berkaitan dengan orang alami yang diidentifikasi atau dapat diidentifikasi, termasuk 'data pribadi' dan 'informasi pribadi' sebagaimana istilah–istilah tersebut didefinisikan dalam Undang–Undang Perlindungan Data yang diproses Tencent berdasarkan Perjanjian untuk menyediakan Layanan;
"**Pemrosesan**" mengacu pada melakukan operasi atau serangkaian operasi apa pun pada Data Pribadi, termasuk pengumpulan, penggunaan, penyimpanan, atau pengungkapan apa pun, atau sebagaimana didefinisikan dalam Undang–Undang Perlindungan Data yang relevan;
"**Pemroses**" mengacu pada seseorang yang Memproses Data Pribadi atas nama satu atau lebih Pengontrol, termasuk sebagaimana berlaku setiap "penyedia layanan" atau "kontraktor" sebagaimana istilah tersebut didefinisikan oleh CCPA;
"**Sub–Prosesor**" Mengacu pada Afiliasi Tencent atau pihak ketiga yang ditunjuk dari waktu ke waktu oleh Tencent untuk Memproses Data Pribadi atas namanya sesuai dengan klausul 7.4;
"**Badan Pengawas**" mengacu pada badan pengatur yang memiliki yurisdiksi kompeten sehubungan dengan Undang–Undang Perlindungan Data;
"**Tencent Cloud**" mengacu pada entitas yang memasok layanan kepada Organisasi, sebagaimana ditentukan dalam Ketentuan Layanan;
"**Tencent Cloud Portal**" mengacu pada portal pelanggan yang memiliki akses Organisasi setelah menyelesaikan proses pendaftaran untuk Tencent Cloud;
"**Kebijakan Privasi Tencent Cloud**" mengacu pada kebijakan yang terletak di Kebijakan Privasi, sebagaimana diperbarui oleh Tencent dan diberitahukan kepada Organisasi dari waktu ke waktu;
"**Kebijakan Keamanan Tencent**" mengacu pada langkah–langkah teknis dan organisasi yang wajar dan tepat yang ditentukan oleh Tencent dari waktu ke waktu, untuk melindungi Data Pribadi terhadap akses, Pemrosesan, penghapusan, kehilangan, atau penggunaan yang tidak sah atau tidak disengaja. Langkah–langkah tersebut akan mencakup langkah–langkah yang ditetapkan dalam Klausul Transfer Pengontrol–Pemroses (jika ada);
"**Ketentuan Layanan**" mengacu pada istilah yang terdapat di Ketentuan Layanan; dan
"**Negara Ketiga**" Mengacu pada semua negara di luar lingkup undang–undang perlindungan data Wilayah Ekonomi Eropa ("**EEA**"), tidak termasuk negara–negara yang disetujui sebagai menyediakan perlindungan untuk Data Pribadi yang memadai oleh Komisi Eropa dari waktu ke waktu, yang pada tanggal Perjanjian ini termasuk Andorra, Argentina, Kanada, Kepulauan Faroe, Guernsey, Isle of Man, Israel, Jersey, Selandia Baru, Swiss, dan Uruguay.
"**Undang–Undang Privasi A.S.**" berarti Undang–Undang Privasi Konsumen California, sebagaimana diubah oleh Undang–Undang Hak Privasi California (California Privacy Rights Act, "CCPA"), Undang–Undang Privasi

Colorado, Undang–Undang Privasi Data Connecticut, Undang–Undang Privasi Konsumen Utah, dan Undang–Undang Perlindungan Data Konsumen Virginia;

Cakupan Perjanjian

Adendum ini berlaku jika Anda telah masuk ke dalam Ketentuan Layanan untuk penyediaan layanan oleh Tencent Cloud. Adendum berlaku untuk Pemrosesan Data Pribadi yang merupakan Konten. Data Pribadi yang merupakan Informasi Administratif Diproses sesuai dengan Kebijakan Privasi Tencent Cloud dan Adendum ini tidak berlaku untuk Pemrosesan Informasi Administratif.

Otorisasi untuk Memproses Data Pribadi

1. Para pihak mengakui bahwa dalam pelaksanaan kewajibannya berdasarkan Perjanjian, Tencent dapat Memproses Data Pribadi sehubungan dengan penyimpanan, akses, dan Pemrosesan Konten oleh Organisasi sebagai bagian dari penyediaan Tencent Cloud. Tujuan dari DPSA ini adalah untuk menetapkan kewajiban masing–masing pihak dalam kaitannya dengan Pemrosesan tersebut.
2. Masing–masing pihak menjamin kepada pihak lain bahwa mereka akan mematuhi semua Undang–Undang Perlindungan Data yang berlaku untuk itu sehubungan dengan Data Pribadi.

Pengontrol dan Pemroses

Tencent dan Organisasi mengakui bahwa Organisasi adalah Pengontrol dan Tencent adalah Pemroses sehubungan dengan Data Pribadi.

Wilayah Layanan

1. Berdasarkan klausul 5.2, di mana Organisasi telah memilih Wilayah Layanan sesuai dengan Perjanjian, Tencent hanya akan Memproses Data Pribadi di Wilayah Layanan tersebut.
2. Organisasi mengakui dan menyetujui bahwa Tencent dapat, untuk alasan operasional, peraturan atau lainnya, perlu mengubah lokasi Pemrosesannya dari waktu ke waktu, asalkan pemrosesan Data Pribadi apa pun di tempat selain Wilayah Layanan pilihan Organisasi akan dianggap sebagai "perubahan material" yang ditangani sesuai dengan Perjanjian.
3. Organisasi mengakui dan menyetujui bahwa Entitas Kontraktor Tencent yang tercantum dalam Ketentuan Layanan mungkin bukan entitas yang memiliki atau mengontrol Data Pelanggan, termasuk Data Pribadi, sehingga data tersebut mungkin disimpan dan diproses di Wilayah Layanan yang dipilih. Jika Organisasi memberikan informasi yang tidak memerlukan pemilihan Wilayah Layanan, seperti informasi terkait akun, Tencent dapat memproses dan menyimpan informasi tersebut di lokasi mana pun.

Kewajiban Tencent

1. Sejauh kegiatannya memproses Data Pribadi atas nama Organisasi, Tencent akan:

   a. Memproses Data Pribadi hanya untuk tujuan terbatas dan ditentukan dalam melakukan Layanan, sesuai dengan instruksi tertulis Organisasi (yang akan mencakup ketentuan DPSA ini setiap instruksi yang

diberikan melalui konsol administratif Organisasi), dan Kebijakan Keamanan Tencent, dan memberi tahu Organisasi segera jika tidak dapat mematuhi DPSA ini atau persyaratannya;
b. mengembalikan atau (atas permintaan tertulis Organisasi) dengan aman menghancurkan semua Data Pribadi yang dimilikinya (termasuk semua salinan cadangan), kecuali jika dilarang melakukannya oleh Hukum yang Berlaku;
c. segera memberi tahu Organisasi, setelah menyadari, tentang:

- perintah pengadilan atau proses hukum lainnya atau permintaan atau tuntutan apa pun oleh Badan Pengawas, regulator, pejabat atau kementerian pemerintah lainnya, badan berwenang, atau agen untuk memperoleh atau mengakses Data Pribadi apa pun, kecuali pemberitahuan tersebut dilarang oleh Hukum yang Berlaku;
- Pelanggaran Data;
- setiap keluhan, komunikasi, atau permintaan material yang berkaitan dengan kewajiban Tencent berdasarkan Undang–Undang Perlindungan Data; dan
- setiap instruksi yang diterima dari Organisasi sehubungan dengan Data Pribadi, yang atas kebijaksanaan Tencent dapat melanggar Hukum yang Berlaku, termasuk Undang–Undang Perlindungan Data, dari yurisdiksi yang sesuai;

d. memastikan bahwa Data Pribadi hanya dapat diakses oleh orang–orang yang berwenang yang terlibat oleh Tencent dan, tunduk pada klausul 8, hanya dapat diakses oleh Sub–Prosesor dan personel Sub–Prosesor tersebut yang berwenang dan yang perlu memiliki akses ke Data Pribadi untuk melakukan kewajiban Tencent berdasarkan Perjanjian;
e. memastikan bahwa personel yang terlibat dan diberi wewenang olehnya untuk Memproses Data Pribadi telah berkomitmen untuk kerahasiaan atau berada di bawah kewajiban kerahasiaan hukum yang sesuai, dan memastikan bahwa kewajiban yang sama untuk perlindungan data berdasarkan DPSA ini dan instruksi Organisasi dipatuhi oleh orang–orang tersebut, dengan mempertimbangkan sifat Pemrosesan;
f. mematuhi Persyaratan Khusus Yurisdiksi yang berlaku; dan
g. di mana hukum yurisdiksi yang relevan mengharuskannya:

- menerapkan langkah–langkah keamanan teknis dan organisasi yang tepat sejauh yang dapat dipraktikkan, untuk tujuan memberikan bantuan yang wajar kepada Organisasi dalam hal tersebut untuk mematuhi kewajibannya, termasuk, sebagaimana mestinya dan berlaku di yurisdiksi yang relevan: (i) penyamaran atau de–identifikasi Data Pribadi; (ii) memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan sistem dan layanan Pemrosesan yang sedang berlangsung; (iii) memulihkan ketersediaan dan akses ke Data Pribadi secara tepat waktu jika terjadi insiden fisik atau teknis; dan (iv) secara teratur menguji, menilai, dan mengevaluasi efektivitas langkah–langkah teknis dan organisasi untuk memastikan keamanan Pemrosesan;
- dengan mempertimbangkan sifat Pemrosesan, membantu Organisasi dengan langkah–langkah teknis dan organisasi yang tepat, sejauh yang dianggap praktis, untuk pemenuhan kewajiban Organisasi untuk menanggapi permintaan untuk melaksanakan hak–hak Subjek Data yang ditetapkan dalam Undang–Undang Perlindungan Data;
- membantu Organisasi dalam memastikan kepatuhan terhadap kewajiban untuk: (i) menerapkan

langkah–langkah keamanan teknis dan organisasi yang tepat; (ii) memberitahukan (jika perlu) Pelanggaran Data kepada Badan Pengawas, Subjek Data yang relevan, dan orang lain yang diperlukan berdasarkan Undang–Undang Perlindungan Data tersebut, dalam kasus di mana pemberitahuan dan pelaporan tersebut diperlukan berdasarkan Undang–Undang Perlindungan Data yang relevan; dan (iii) melakukan penilaian dampak perlindungan data dan, jika diperlukan, konsultasi sebelumnya dengan Otoritas Pengawas; dan

- segera memberi tahu Organisasi secara tertulis setelah mengetahui akses yang tidak benar, tidak sah, atau melanggar hukum ke, penggunaan, atau pengungkapan, Data Pribadi yang Diproses oleh Tencent di bawah atau sehubungan dengan DPSA ini. Tencent berkewajiban untuk menyediakan Organisasi dengan semua informasi yang diperlukan secara wajar untuk mematuhi kewajiban Organisasi sesuai dengan Undang–Undang Perlindungan Data.

2. Tencent akan memberi tahu Organisasi jika, menurut pendapatnya, instruksi Organisasi melanggar Undang–Undang Perlindungan Data.

Kewajiban Organisasi

1. Organisasi mewakili, menjamin, dan berjanji kepada Tencent selama Jangka Waktu bahwa:

   a. Data Pribadi telah dan akan dikumpulkan sesuai dengan Undang–Undang Perlindungan Data;
   b. semua instruksi dari Organisasi ke Tencent akan mematuhi Undang–Undang Perlindungan Data; dan
   c. transfer Data Pribadi ke Tencent, dan (sejauh Tencent bertindak sebagai pemroses data sehubungan dengan Data Pribadi tersebut) Pemrosesan Data Pribadi oleh Tencent sebagaimana diinstruksikan oleh Organisasi atau (sejauh Tencent bertindak sebagai pengontrol data sehubungan dengan Data Pribadi tersebut) penerimaan dan penggunaan Data Pribadi oleh Tencent, Pengolahan, dan penggunaan Data Pribadi seperti yang tercantum di DPSA, disetujui oleh Subjek Data yang relevan (di mana diperlukan oleh hukum) dan sebaliknya diizinkan oleh dan sesuai dengan Undang–Undang Perlindungan Data.
2. Organisasi setuju bahwa mereka akan mengganti rugi dan membebaskan Tencent atas permintaan dari dan terhadap semua klaim, kewajiban, biaya, biaya, kerugian atau kerusakan (termasuk kerugian konsekuensial, kehilangan laba, rugi reputasi, dan semua bunga, penalti, dan biaya serta pengeluaran profesional lainnya) yang dikeluarkan oleh Tencent yang timbul secara langsung atau tidak langsung dari pelanggaran klausul ini.
3. Di mana Tencent menghadapi klaim aktual atau potensial yang timbul dari atau terkait dengan pelanggaran Undang–Undang Perlindungan Data yang berkaitan dengan Data Pribadi yang diproses sesuai dengan DPSA ini, Organisasi akan segera memberikan semua materi dan informasi yang diminta secara wajar oleh Tencent yang relevan dengan pembelaan klaim tersebut.
4. Jika Organisasi menyadari adanya Pelanggaran Data aktual atau yang dicurigai terkait dengan Perjanjian, Organisasi harus:

   a. mengambil langkah–langkah yang wajar untuk melaksanakan, dalam waktu 30 hari, penilaian untuk menentukan apakah Pelanggaran Data dapat diberitahukan berdasarkan Undang–Undang Perlindungan Data dan segera memberi tahu Tencent secara tertulis tentang hasil penilaian;

b. jika Organisasi memberi tahu Tencent bahwa mereka menganggap Pelanggaran Data dapat diberi tahu berdasarkan Undang–Undang Perlindungan Data:

- Organisasi harus menyiapkan draf pernyataan pemberitahuan sehubungan dengan Pelanggaran Data yang diperlukan berdasarkan Undang–Undang Perlindungan Data ("Pernyataan Pemberitahuan") dan memberikan draf Pernyataan Pemberitahuan kepada Tencent untuk disetujui sebelum pengungkapan kepada regulator perlindungan data yang berlaku, Subjek Data, atau orang lain;
- Tencent akan memberikan pemberitahuan kepada Organisasi secara tertulis:
  - setiap perubahan yang diperlukan Tencent terhadap draf Pernyataan Pemberitahuan dan Organisasi harus memasukkan semua perubahan tersebut ke dalam draf Pernyataan Pemberitahuan; atau
  - bahwa Tencent menyetujui draf Pernyataan Pemberitahuan; dan
- setelah persetujuan Tencent atas rancangan Pernyataan Pemberitahuan, Organisasi harus memberikan salinan Pernyataan Pemberitahuan yang disetujui kepada regulator perlindungan data yang berlaku, Subjek Data dan orang lain sebagaimana dipersyaratkan oleh Undang–Undang Perlindungan Data; dan
- tidak, dan harus memastikan bahwa Afiliasinya dan personel masing–masing tidak, membuat pernyataan publik atau pengungkapan yang berkaitan dengan dugaan atau pelanggaran data aktual tanpa persetujuan tertulis sebelumnya dari Tencent.

Penunjukan Sub–Prosesor

1. Tencent dapat mengizinkan Sub–Prosesor apa pun untuk Memproses Data Pribadi atas namanya asalkan, di mana (dan sejauh) yang dipersyaratkan oleh Undang–Undang Perlindungan Data, Tencent menandatangani perjanjian tertulis dengan Sub–Prosesor yang secara substansial sama dengan yang diperlukan oleh Undang–Undang Perlindungan Data, Tencent menandatangani perjanjian tertulis dengan Sub–Prosesor yang secara substansial sama dengan yang diperlukan di DPSA ini. Organisasi dengan ini memberikan otorisasi tertulis umum Tencent untuk melibatkan Sub–Prosesor yang terdaftar di Tencent Cloud. Pihak Ketiga, tunduk pada persyaratan klausul 8 ini.
2. Tencent harus, sejauh Data Pribadi tunduk pada Undang–Undang Perlindungan Data yang mewajibkan pemberitahuan tersebut, menginformasikan Organisasi melalui email (dan melalui Portal Cloud Tencent) tentang perubahan yang dimaksudkan mengenai penambahan atau penggantian Sub–Prosesor. Dalam kasus seperti itu, Organisasi akan memiliki empat belas (14) hari sejak tanggal penerimaan pemberitahuan untuk menyetujui atau menolak perubahan tersebut. Jika tidak ada tanggapan dari Organisasi, Sub–Prosesor akan dianggap diterima. Jika Organisasi menolak sub–prosesor pengganti, Tencent dapat mengakhiri Perjanjian dengan segera pada pemberitahuan tertulis kepada Organisasi.
3. Dalam hal Tencent melibatkan Sub–Prosesor untuk melakukan kegiatan Pemrosesan tertentu atas nama Organisasi, di mana Sub–Prosesor tersebut gagal memenuhi kewajiban perlindungan datanya, Tencent akan tetap bertanggung jawab penuh berdasarkan Undang–Undang Perlindungan Data kepada Organisasi untuk pelaksanaan kewajiban Sub–Prosesor tersebut.

MODUL

Modul berikut akan berlaku dan dimasukkan dengan referensi ke dalam DPSA ini jika Anda menggunakan Fitur tertentu (sebagaimana didefinisikan dalam setiap Modul yang relevan).

1. Tencent Push Notification Service.
2. Anti-Cheat Expert.
3. Web Application Firewall.
4. Game Multimedia Engine.
5. Anti-DDoS.
6. Face Recognition.
7. StreamLive.
8. StreamPackage.
9. Cloud Object Storage.
10. Cloud Native Database TDSQL-C.
11. Tencent Cloud Elastic Microservice.
12. TencentDB for CTSDB.
13. Private DNS.
14. TencentDB for Tendis.
15. Database Management Center.
16. Event Bridge.
17. TencentCloud Lighthouse.
18. Instant Messaging.
19. Edge Computing Machine.
20. Data Security Center.
21. Tencent Cloud TI Platform.
22. Cloud Data Warehouse.
23. Vulnerability Scan Service.
24. IoT Hub.
25. Tencent Distributed Message Queue.
26. Risk Control Engine.
27. TencentCloud EdgeOne.
28. eKYC.
29. Tencent Managed Service for Prometheus.
30. Video on Demand.
31. Tencent Cloud Automation Tools.

32. HTTPDNS.
33. Tencent Effect SDK.
34. Text To Speech.
35. Automatic Speech Recognition.
36. Cloud Streaming Services.
37. Tencent Real-Time Communication.
38. Real User Monitoring.
39. Customer Identity and Access Management.
40. Cloud Application Rendering.
41. OCR.
42. Captcha.
43. Tencent Machine Translation.
44. Data Lake Compute.
45. Tencent Ecard.
46. Tencent Cloud Firewall.
47. User Generated Short Video SDK.
48. Key Management Service.
49. App Flow.
50. Low-code Interactive Classroom.
51. Tencent Container Security Service.
52. Cloud Automated Testing.
53. Cloud Log Service.
54. Tencent Interactive Whiteboard.
55. Bastion Host.
56. Cloud Workload Protection Platform.
57. Control Center.
58. Intelligent Music Platform.
59. Face Fusion.
60. Data Security Audit.
61. Cloud Dedicated Cluster.
62. Tencent Cloud WeData.
63. CloudApp.
64. Video Creation Large Model.
65. Cloud HDFS.

66. Security Service Platform.
67. Business Intelligence.

Persyaratan khusus yurisdiksi

Eropa

1. Tencent setuju bahwa mereka tidak akan Memproses Data Pribadi UE di Negara Ketiga kecuali jika Tencent mematuhi kewajiban pengimpor data yang ditetapkan dalam Klausul Transfer Pengontrol–Pemroses.
2. Sejauh konflik antara Klausul Transfer Pengontrol–Pemroses dan isi DPSA ini, Klausul Transfer Pengontrol–Pemroses akan berlaku sehubungan dengan Data Pribadi UE.
3. Untuk tujuan Klausul Transfer Pengontrol–Pemroses, ketentuan tambahan berikut akan berlaku:

   a. para pihak setuju untuk mematuhi Klausul Transfer Pengontrol–Pemroses tanpa modifikasi;
   b. nama dan alamat Organisasi dan Tencent akan dianggap dimasukkan ke dalam Klausul Transfer Pengontrol–Pemroses dan untuk tujuan Klausul Transfer Pengontrol–Pemroses;
   c. Organisasi adalah pengekspor data dan Tencent, atau Afiliasi Tencent yang berlaku, adalah pengimpor data sebagaimana didefinisikan dalam Klausul Transfer Pengontrol–Pemroses; dan
   d. Tanda tangan masing–masing pihak untuk DPSA ini akan dianggap sebagai tanda tangan untuk persyaratan yang terkandung dalam Klausul Transfer Pengontrol–Pemroses.
4. Jika diwajibkan oleh undang–undang atau prosedur peraturan dari yurisdiksi mana pun, para pihak akan mengeksekusi atau melaksanakan kembali klausul yang terkandung dalam Klausul Transfer Pengontrol–Pemroses sebagai dokumen terpisah yang menetapkan transfer Data Pribadi yang diusulkan dengan cara yang mungkin diperlukan.

Korea Selatan

1. Jika dan sejauh Kebijakan Keamanan Tencent tidak cukup untuk memenuhi persyaratan yang berlaku berdasarkan undang–undang dan peraturan privasi Korea, Tencent akan mengambil langkah–langkah tambahan dari waktu ke waktu untuk mematuhi persyaratan tersebut (sebagaimana berlaku untuk penerima Data Pribadi di luar negeri), termasuk:

   a. Pasal 28 dan 63 Undang–Undang tentang Promosi Pemanfaatan Jaringan Informasi dan Komunikasi dan Perlindungan Informasi ("**Undang–Undang Jaringan ICT**");
   b. Pasal 15 dan 67 dari Keputusan Penegakan yang diumumkan berdasarkan Undang–Undang Jaringan ICT;
   c. Pedoman untuk Langkah–Langkah Teknis dan Administratif untuk Perlindungan Informasi Pribadi (dikeluarkan oleh Komisi Komunikasi Korea);
   d. Pasal 29 Undang–Undang Perlindungan Informasi Pribadi ("**PIPA**");
   e. Pasal 30 dari Keputusan Penegakan yang diumumkan berdasarkan PIPA;
   f. Pedoman untuk Langkah–Langkah Keamanan untuk Keselamatan Informasi Pribadi (dikeluarkan oleh Kementerian Dalam Negeri dan Keselamatan), karena hal tersebut di atas dapat diubah dan/atau ditambah dari waktu ke waktu.

2. Tencent akan:

   a. menggunakan Data Pribadi hanya untuk tujuan dan dalam lingkup pekerjaan yang dipercayakan;
   b. setuju untuk tunduk pada pelatihan dan pengawasan oleh Organisasi Tencent dalam menangani Data Pribadi; dan
   c. setuju untuk tunduk pada pengawasan dan audit oleh badan pengatur terkait.
3. Tencent akan memberikan kompensasi kepada Organisasi dan subjek data yang relevan untuk setiap dan semua kerusakan, kewajiban, biaya, dan biaya yang timbul dari pelanggaran kewajiban Tencent berdasarkan DPSA ini atau berdasarkan Hukum yang Berlaku.

Undang-Undang Privasi A.S.

1. Sejauh yang diwajibkan oleh Undang-Undang Privasi A.S. yang berlaku, dan atas permintaan atau pemberitahuan tertulis yang wajar:

   a. Organisasi dapat mengambil langkah-langkah yang wajar dan sesuai untuk memastikan bahwa Tencent menggunakan Data Pribadi dengan cara yang sesuai dengan kewajiban Organisasi berdasarkan Undang-Undang Privasi A.S. yang berlaku;
   b. Sejauh Organisasi secara wajar meyakini bahwa Tencent menggunakan Data Pribadi yang melanggar Undang-Undang Privasi A.S. yang berlaku, Organisasi dapat mengambil langkah-langkah yang wajar dan sesuai untuk menghentikan dan memulihkan penggunaan yang tidak sah tersebut;
   c. Tencent akan menyediakan informasi yang dimiliki Tencent kepada Organisasi yang diperlukan untuk menunjukkan kepatuhan Tencent terhadap kewajibannya berdasarkan Undang-Undang Privasi A.S.
   d. Tencent akan mengizinkan dan bekerja sama dengan penilaian tahunan yang wajar oleh Organisasi, atau auditor yang ditunjuk oleh Organisasi, atas biaya Organisasi dan hanya setelah para pihak mencapai kesepakatan tentang ruang lingkup penilaian, tentang kepatuhan Tencent terhadap kewajibannya berdasarkan Undang-Undang Privasi A.S. yang berlaku. Selain itu, Tencent dapat mengatur agar auditor yang berkualifikasi dan independen melakukan penilaian terhadap kebijakan Tencent dan tindakan teknis dan organisasi untuk mendukung kewajibannya berdasarkan Undang-Undang Privasi A.S. yang berlaku menggunakan standar pengendalian atau kerangka kerja dan prosedur penilaian yang sesuai dan diterima untuk penilaian tersebut. Tencent akan memberikan laporan penilaian tersebut kepada Organisasi atas permintaan yang wajar.
2. Para Pihak wajib, dengan mempertimbangkan konteks Pemrosesan, menerapkan langkah-langkah teknis dan organisasi yang tepat yang dirancang untuk memberikan tingkat keamanan yang sesuai dengan risiko dan menetapkan pembagian tanggung jawab yang jelas di antara mereka untuk menerapkan langkah-langkah tersebut. Sejauh diwajibkan oleh Undang-Undang Privasi A.S. yang berlaku, Tencent akan memberikan tingkat perlindungan privasi yang sama seperti yang diwajibkan oleh undang-undang tersebut.
3. Tencent dilarang:

   a. Menjual dan Membagikan Data Pribadi;
   b. menyimpan, menggunakan, atau mengungkapkan Data Pribadi untuk tujuan apa pun selain untuk tujuan khusus dalam menjalankan Layanan;
   c. menyimpan, menggunakan, atau mengungkapkan Data Pribadi di luar hubungan bisnis langsung antara

Tencent dengan Organisasi; dan
d. menggabungkan Data Pribadi yang diterima dari, atau atas nama, Organisasi dengan Data Pribadi yang dapat dikumpulkan dari interaksi terpisah Tencent dengan individu yang terkait dengan Data Pribadi tersebut atau dari sumber lain, kecuali sejauh diizinkan oleh Undang–Undang Privasi A.S. Untuk tujuan bagian Undang–Undang Privasi A.S. ini, “Jual”, “Bagikan”, dan istilah yang serupa lainnya akan memiliki makna yang diberikan kepada mereka dalam Undang–Undang Privasi A.S.

Makau

1. Penunjukan Tencent sebagai Pemroses, serta penunjukan sub–prosesor di mana (dan sejauh) diizinkan dalam Perjanjian ini, harus diberitahukan oleh Organisasi ke kantor perlindungan data lokal (GPDP – Gabinete para a Protecção de Dados Pessoais).
2. Tencent berhak untuk meminta Organisasi secara wajar memberikan bukti kepatuhan terhadap instruksi berdasarkan undang–undang perlindungan data Macau yang relevan, termasuk pemberitahuan tersebut berdasarkan bagian 1 di atas.
3. Organisasi harus secara tegas menginformasikan Tencent, secara tertulis, dalam hal pemrosesan data sensitif, sebagaimana didefinisikan dalam pasal 7 Undang–Undang Perlindungan Data Makau (UU n. 8/2005), dan harus memastikan kepatuhan dengan persyaratan khusus yang diatur dalam undang–undang perlindungan data Macau untuk pemrosesan data tersebut.

Klausul Transfer Pengontrol–Pemroses

Untuk tujuan Pasal 26 (2) Petunjuk 95/46 / EC untuk transfer data pribadi ke pemroses yang didirikan di negara ketiga yang tidak menjamin tingkat perlindungan data memadai:
Nama organisasi pengekspor data: Ini adalah Organisasi yang telah masuk ke dalam Perjanjian, atau jika Perjanjian dimasukkan dengan individu yang tidak bertindak atas nama Organisasi, individu tersebut.
("**pengekspor data**")
Dan
Nama organisasi pengimpor data: Entitas kontraktor yang ditentukan dalam bagian 1.2 dari Ketentuan Layanan.
("**pengimpor data**")
masing–masing "**pihak**"; bersama–sama "**para pihak**",
TELAH MENYETUJUI Klausul Kontrak berikut ("**Klausul**") Untuk menambahkan perlindungan yang memadai sehubungan dengan perlindungan privasi dan hak–hak dasar dan kebebasan individu untuk transfer data pribadi oleh pengekspor data ke pengimpor data yang ditentukan dalam Lampiran 1.

Definisi

Untuk tujuan Klausul:
a. 'data pribadi', 'kategori data khusus', 'proses/pemrosesan', 'pengontrol', 'pemroses', 'subjek data' dan 'badan pengawas' akan memiliki arti yang sama seperti dalam Arahan 95/46 / EC parlemen Eropa dan Dewan 24 Oktober 1995 tentang perlindungan individu sehubungan dengan pemrosesan data pribadi dan pada pergerakan bebas data tersebut;

b. 'pengekspor data' mengacu pada pengontrol yang mentransfer data pribadi;
c. 'pengimpor data' mengacu pada pemroses yang setuju untuk menerima dari data pribadi pengekspor data yang dimaksudkan untuk diproses atas namanya setelah transfer sesuai dengan instruksinya dan ketentuan Klausul dan yang tidak tunduk pada sistem negara ketiga yang memastikan perlindungan memadai sesuai artinya dalam Pasal 25 (1) Dari Arahan 95/46 / EC;
d. 'sub–prosesor' mengacu pada setiap pemroses yang terlibat oleh pengimpor data atau oleh sub–prosesor lain dari pengimpor data yang setuju untuk menerima dari pengimpor data atau dari sub–pemroses lain dari data pribadi pengimpor data yang secara eksklusif ditujukan untuk kegiatan pemrosesan yang akan dilakukan atas nama pengekspor data setelah transfer sesuai dengan instruksinya, ketentuan Klausul dan ketentuan subkontrak tertulis;
e. 'undang–undang perlindungan data yang berlaku' mengacu pada undang–undang yang melindungi hak–hak dasar dan kebebasan individu dan, khususnya, hak privasi mereka sehubungan dengan pemrosesan data pribadi yang berlaku untuk pengontrol data di Negara Anggota tempat pengekspor data didirikan;
f. 'Langkah–langkah keamanan teknis dan organisasi' mengacu pada langkah–langkah yang bertujuan melindungi data pribadi terhadap kerusakan yang tidak disengaja atau melanggar hukum atau kehilangan yang tidak disengaja, perubahan, pengungkapan atau akses yang tidak sah, khususnya di mana pemrosesan melibatkan transmisi data melalui jaringan, dan terhadap semua bentuk pemrosesan yang melanggar hukum lainnya.

Detail transfer

Detail transfer dan khususnya kategori khusus data pribadi jika berlaku ditentukan dalam Lampiran 1 yang merupakan bagian integral dari Klausul.

Klausul penerima manfaat pihak ketiga

1. Subjek data dapat menegakkan terhadap pengekspor data Klausul ini, Klausul 4(b) hingga 4(i), Klausul 5(a) hingga 5(e) dan 5(g) hingga 5(j), Klausul 6.1 dan 6.2, Klausul 7, Klausul 8.2 dan Klausul 9 hingga 12 sebagai penerima pihak ketiga.
2. Subjek data dapat menegakkan terhadap pengimpor data Klausul ini, Klausul 5(a) hingga 5(e) dan 5(g), Klausul 6, Klausul 7, Klausul 8.2 dan Klausul 9 hingga 12, dalam kasus di mana pengekspor data telah menghilang secara faktual atau tidak ada lagi dalam hukum kecuali entitas penerus telah mengasumsikan seluruh kewajiban hukum pengekspor data dengan kontrak atau dengan operasi hukum, sebagai akibatnya dibutuhkan hak dan kewajiban pengekspor data, dalam hal ini subjek data dapat menegakkannya terhadap entitas tersebut.
3. Subjek data dapat menegakkan terhadap sub–prosesor Klausul ini, Klausul 5(a) hingga 5(e) dan 5(g), Klausul 6, Klausul 7, Klausul 8.2 dan Klausul 9 hingga 12, dalam kasus di mana pengekspor data dan pengimpor data telah menghilang secara faktual atau tidak ada lagi dalam hukum atau telah bangkrut, kecuali entitas penerus telah mengasumsikan seluruh kewajiban hukum pengekspor data dengan kontrak atau dengan operasi hukum, sebagai akibatnya dibutuhkan hak dan kewajiban pengekspor data, dalam

hal ini subjek data dapat menegakkannya terhadap entitas tersebut. Tanggung jawab pihak ketiga dari sub–prosesor tersebut akan terbatas pada operasi pemrosesannya sendiri berdasarkan Klausul.

4. Para pihak tidak keberatan dengan subjek data yang diwakili oleh asosiasi atau badan lain jika subjek data secara tegas menginginkannya dan jika diizinkan oleh hukum negara.

Kewajiban pengekspor data

Pengekspor data setuju dan menjamin:
a. bahwa pemrosesan, termasuk transfer itu sendiri, dari data pribadi telah dan akan terus dilakukan sesuai dengan ketentuan yang relevan dari undang–undang perlindungan data yang berlaku (dan, jika berlaku, telah diberitahukan kepada otoritas terkait dari Negara Anggota di mana pengekspor data didirikan) dan tidak melanggar ketentuan yang relevan dari Negara tersebut;
b. bahwa ia telah menginstruksikan dan selama durasi layanan pemrosesan data pribadi akan menginstruksikan pengimpor data untuk memproses data pribadi yang ditransfer hanya atas nama pengekspor data dan sesuai dengan undang–undang perlindungan data dan Klausul yang berlaku;
c. bahwa pengimpor data akan memberikan jaminan yang cukup sehubungan dengan langkah–langkah keamanan teknis dan organisasi yang ditentukan dalam Lampiran 2 untuk kontrak ini;
d. bahwa setelah penilaian persyaratan undang–undang perlindungan data yang berlaku, langkah–langkah keamanan yang tepat untuk melindungi data pribadi terhadap kerusakan disengaja atau melanggar hukum atau kehilangan disengaja, perubahan, pengungkapan atau akses yang tidak sah, khususnya di mana pengolahan melibatkan transmisi data melalui jaringan, dan terhadap semua bentuk pengolahan yang melanggar hukum lainnya, dan bahwa langkah–langkah ini memastikan tingkat keamanan yang sesuai dengan risiko yang disajikan oleh pengolahan dan sifat data yang harus dilindungi dengan memperhatikan teknologi terkini dan biaya implementasinya;
e. bahwa hal itu akan memastikan kepatuhan terhadap langkah–langkah keamanan;
f. bahwa, jika transfer melibatkan kategori data khusus, subjek data telah diinformasikan atau akan diinformasikan sebelum, atau sesegera mungkin setelahnya, transfer bahwa datanya dapat dikirimkan ke negara ketiga yang tidak memberikan perlindungan yang memadai dalam arti Arahan 95/46/EC;
g. untuk meneruskan pemberitahuan yang diterima dari pengimpor data atau sub–prosesor sesuai dengan Klausul 5 (b) dan Klausul 8.3 kepada otoritas pengawas perlindungan data jika pengekspor data memutuskan untuk melanjutkan transfer atau untuk mencabut penangguhan;
h. untuk menyediakan subjek data atas permintaan salinan Klausul, dengan pengecualian Lampiran 2, dan deskripsi ringkasan dari langkah–langkah keamanan, serta salinan kontrak apa pun untuk layanan sub–pemrosesan yang harus dibuat sesuai dengan Klausul, kecuali Klausul atau kontrak berisi informasi komersial, yang dalam hal ini dapat menghapus informasi komersial tersebut;
i. bahwa, dalam hal sub–pemrosesan, aktivitas pemrosesan dilakukan sesuai dengan Klausul 11 oleh sub–prosesor yang menyediakan setidaknya tingkat perlindungan yang sama untuk data pribadi dan hak subjek data sebagai pengimpor data berdasarkan Klausul; dan
j. bahwa hal itu akan memastikan kepatuhan dengan Klausul 4 (a) hingga 4 (i).

Kewajiban pengimpor data

Pengimpor data setuju dan menjamin:
a. untuk memproses data pribadi hanya atas nama pengekspor data dan sesuai dengan instruksi dan Klausulnya; jika tidak dapat memberikan kepatuhan tersebut karena alasan apa pun, ia setuju untuk segera menginformasikan pengekspor data ketidakmampuannya untuk mematuhi, dalam hal ini pengekspor data berhak untuk menangguhkan transfer data dan/atau mengakhiri kontrak;
b. bahwa ia tidak memiliki alasan untuk percaya bahwa undang–undang yang berlaku mencegahnya memenuhi instruksi yang diterima dari pengekspor data dan kewajibannya berdasarkan kontrak dan bahwa jika terjadi perubahan dalam undang–undang ini yang kemungkinan memiliki efek buruk yang substansial pada jaminan dan kewajiban yang diberikan oleh Klausul, ia akan segera memberi tahu perubahan kepada pengekspor data segera setelah diketahui, dalam hal ini pengekspor data berhak untuk menangguhkan transfer data dan/atau mengakhiri kontrak;
c. bahwa ia telah menerapkan langkah–langkah keamanan teknis dan organisasi yang ditentukan dalam Lampiran 2 sebelum memproses data pribadi yang ditransfer;
d. bahwa ia akan segera memberi tahu pengekspor data tentang:

- setiap permintaan yang mengikat secara hukum untuk pengungkapan data pribadi oleh badan penegak hukum kecuali jika dilarang, seperti larangan di bawah hukum pidana untuk menjaga kerahasiaan penyelidikan penegakan hukum,
- setiap akses yang tidak disengaja atau tidak sah, dan
- setiap permintaan yang diterima langsung dari subjek data tanpa menanggapi permintaan itu, kecuali jika telah diberi wewenang untuk melakukannya;

e. untuk menangani dengan cepat dan benar semua pertanyaan dari pengekspor data yang berkaitan dengan pemrosesan data pribadinya yang tunduk pada transfer dan untuk mematuhi saran dari otoritas pengawas sehubungan dengan pemrosesan data yang ditransfer;
f. atas permintaan pengekspor data untuk menyerahkan fasilitas pemrosesan datanya untuk audit kegiatan pemrosesan yang dicakup oleh Klausul yang akan dilakukan oleh pengekspor data atau badan inspeksi yang terdiri dari anggota independen dan memiliki kualifikasi profesional yang diperlukan yang terikat oleh kewajiban kerahasiaan, dipilih oleh pengekspor data, jika berlaku, sesuai dengan otoritas pengawas;
g. untuk menyediakan subjek data atas permintaan salinan Klausul, atau kontrak apa pun yang ada untuk sub–pemrosesan; kecuali Klausul atau kontrak berisi informasi komersial, yang dalam hal ini dapat menghapus informasi komersial tersebut, dengan pengecualian Lampiran 2 yang akan diganti dengan deskripsi rangkuman tindakan keamanan dalam kasus di mana subjek data tidak dapat memperoleh salinan dari pengekspor data;
h. bahwa, dalam hal sub–pemrosesan, sebelumnya telah memberi tahu pengekspor data dan memperoleh persetujuan tertulis sebelumnya;
i. bahwa layanan pemrosesan oleh sub–prosesor akan dilakukan sesuai dengan Klausul 11;
j. untuk segera mengirim salinan perjanjian sub–prosesor yang disimpulkan berdasarkan Klausul kepada pengekspor data.

Pertanggungjawaban

1. Para pihak setuju bahwa setiap subjek data, yang telah mengalami kerusakan sebagai akibat dari pelanggaran kewajiban sebagaimana dimaksud dalam Klausul 3 atau dalam Klausul 11 oleh pihak atau sub–pemroses mana pun berhak menerima kompensasi dari pengekspor data atas kerusakan yang diderita.
2. Jika subjek data tidak dapat mengajukan klaim kompensasi sesuai dengan Klausul 6.1 terhadap pengekspor data, yang timbul dari pelanggaran oleh pengimpor data atau sub–prosesornya atas kewajiban mereka sebagaimana dimaksud dalam Klausul 3 atau dalam Klausul 11, karena pengekspor data telah menghilang secara faktual atau tidak ada lagi dalam hukum atau telah menjadi bangkrut, Pengimpor data setuju bahwa subjek data dapat mengeluarkan klaim terhadap pengimpor data seolah–olah itu adalah pengekspor data, kecuali entitas penerus telah mengasumsikan seluruh kewajiban hukum pengekspor data dengan kontrak dengan operasi hukum, dalam hal ini subjek data dapat menegakkan hak–haknya terhadap entitas tersebut. Pengimpor data mungkin tidak bergantung pada pelanggaran oleh sub–prosesor atas kewajibannya untuk menghindari tanggung jawabnya sendiri.
3. Jika subjek data tidak dapat mengajukan klaim terhadap pengekspor data atau pengimpor data yang dirujuk dalam Klausul 6.1 dan 6.2, yang timbul dari pelanggaran sub–prosesor atas kewajiban mereka sebagaimana dimaksud dalam Klausul 3 atau dalam Klausul 11, karena pengekspor data dan pengimpor data telah menghilang secara faktual atau tidak ada lagi dalam hukum atau telah menjadi bangkrut, sub–prosesor data setuju bahwa subjek data dapat mengeluarkan klaim terhadap sub–prosesor data terkait operasi pemrosesannya sendiri dalam Klausul seolah–olah itu adalah pengekspor data atau pengimpor data, kecuali entitas penerus telah mengasumsikan seluruh kewajiban hukum pengekspor data atau pengimpor data dengan kontrak dengan operasi hukum, dalam hal ini subjek data dapat menegakkan hak–haknya terhadap entitas tersebut. Tanggung jawab dari sub–prosesor tersebut akan terbatas pada operasi pemrosesannya sendiri berdasarkan Klausul.

Mediasi dan yurisdiksi

1. Pengimpor data setuju bahwa jika subjek data meminta hak penerima pihak ketiga dan/atau mengklaim kompensasi atas kerusakan berdasarkan Klausul, pengimpor data akan menerima keputusan subjek data:

   a. untuk merujuk sengketa ke mediasi, oleh orang yang independen atau, jika berlaku, oleh otoritas pengawas;

   b. untuk merujuk sengketa ke pengadilan di Negara Anggota di mana pengekspor data didirikan.
2. Para pihak setuju bahwa pilihan yang dibuat oleh subjek data tidak akan mengurangi hak substantif atau proseduralnya untuk mencari solusi sesuai dengan ketentuan lain dari hukum nasional atau internasional.

Kerjasama dengan badan pengawas

1. Pengekspor data setuju untuk menyetor salinan kontrak ini dengan badan pengawas jika diminta atau jika penyetoran tersebut diperlukan berdasarkan undang–undang perlindungan data yang berlaku.
2. Para pihak setuju bahwa badan pengawas memiliki hak untuk melakukan audit terhadap pengimpor data, dan sub–prosesor apa pun, yang memiliki ruang lingkup yang sama dan tunduk pada kondisi yang sama

seperti yang akan berlaku untuk audit pengekspor data berdasarkan undang–undang perlindungan data yang berlaku.

3. Pengimpor data akan segera memberi tahu pengekspor data tentang keberadaan undang–undang yang berlaku untuknya atau sub–pemroses apa pun yang mencegah pelaksanaan audit importir data, atau sub–prosesor apa pun, sesuai dengan Klausul 8.2. Dalam kasus seperti itu, pengekspor data berhak untuk mengambil langkah–langkah yang diprediksi dalam Klausul 5 (b).

Hukum yang Mengatur

Klausul akan diatur oleh hukum Negara Anggota di mana pengekspor data didirikan.

Variasi kontrak

Para pihak berjanji untuk tidak membuat variasi atau modifikasi Klausul. Ini tidak menghalangi para pihak untuk menambahkan klausul tentang masalah terkait bisnis jika diperlukan selama mereka tidak bertentangan dengan Klausul.

Sub–pemrosesan

1. Pengimpor data tidak akan melakukan subkontrak untuk salah satu operasi pemrosesannya yang dilakukan atas nama pengekspor data berdasarkan Klausul tanpa persetujuan tertulis sebelumnya dari pengekspor data. Jika pengimpor data melakukan subkontrak atas kewajibannya berdasarkan Klausul, dengan persetujuan pengekspor data, ia akan melakukannya hanya dengan cara perjanjian tertulis dengan sub–prosesor yang memberlakukan kewajiban yang sama pada sub–prosesor seperti yang dikenakan pada pengimpor data berdasarkan Klausul. Jika sub–prosesor gagal memenuhi kewajiban perlindungan data berdasarkan perjanjian tertulis tersebut, pengimpor data akan tetap sepenuhnya bertanggung jawab kepada pengekspor data atas kinerja kewajiban sub–prosesor berdasarkan perjanjian tersebut.
2. Kontrak tertulis sebelumnya antara pengimpor data dan sub–prosesor juga akan menyediakan klausul penerima manfaat pihak ketiga sebagaimana diatur dalam Klausul 3 untuk kasus–kasus di mana subjek data tidak dapat membawa klaim untuk kompensasi sebagaimana dimaksud dalam Klausul 6.1 terhadap pengekspor data atau pengimpor data karena mereka telah menghilang secara faktual atau tidak ada lagi dalam hukum atau telah menjadi bangkrut dan tidak ada entitas penerus yang berasumsi. seluruh kewajiban hukum pengekspor data atau pengimpor data berdasarkan kontrak atau dengan operasi hukum. Tanggung jawab pihak ketiga dari sub–prosesor tersebut akan terbatas pada operasi pemrosesannya sendiri berdasarkan Klausul.
3. Ketentuan yang berkaitan dengan aspek perlindungan data untuk sub–pemrosesan kontrak sebagaimana dimaksud dalam Klausul 11.1 akan diatur oleh hukum Negara Anggota di mana pengekspor data didirikan.
4. Pengekspor data akan menyimpan daftar perjanjian sub–pemrosesan yang disimpulkan berdasarkan Klausul dan diberi tahu oleh pengimpor data sesuai dengan Klausul 5 (j), yang akan diperbarui

setidaknya setahun sekali. Daftar ini akan tersedia bagi badan pengawas perlindungan data pengekspor data.

Kewajiban setelah penghentian layanan pemrosesan data pribadi

1. Para pihak setuju bahwa pada penghentian penyediaan layanan pemrosesan data, pengimpor data, dan sub-prosesor akan, atas pilihan pengekspor data, mengembalikan semua data pribadi yang ditransfer dan salinannya kepada pengekspor data atau akan menghancurkan semua data pribadi dan menyatakan kepada pengekspor data bahwa ia telah melakukannya, kecuali Undang-undang yang dikenakan pada pengimpor data mencegahnya mengembalikan atau menghancurkan semua atau sebagian dari data pribadi yang ditransfer. Dalam hal ini, pengimpor data menjamin bahwa ia akan menjamin kerahasiaan data pribadi yang ditransfer dan tidak akan secara aktif memproses data pribadi yang ditransfer lagi.
2. Pengimpor data dan sub-prosesor menjamin bahwa atas permintaan pengekspor data dan/atau badan pengawas, ia akan menyerahkan fasilitas pemrosesan datanya untuk audit langkah-langkah yang dimaksud dalam Klausul 12.1.

Lampiran 1

Deskripsi Transfer (Pengontrol-Pemroses)

Lampiran ini merupakan bagian dari Klausul dan harus diselesaikan dan ditandatangani oleh para pihak. Negara-negara Anggota dapat melengkapi atau menentukan, sesuai dengan prosedur nasional mereka, setiap informasi tambahan yang diperlukan untuk terkandung dalam Lampiran ini.

Pengekspor data

Pengekspor data adalah Organisasi sebagaimana yang ditentukan dalam Perjanjian, atau jika Perjanjian dimasukkan dengan individu yang tidak bertindak atas nama Organisasi, individu tersebut.

Pengekspor data telah melibatkan pengimpor data untuk menyediakan layanan online seperti yang dijelaskan dalam Perjanjian.

Pengimpor data

Pengimpor data adalah Tencent, sebagaimana didefinisikan dalam Perjanjian, penyedia layanan bernilai tambah Internet terkemuka. Pengimpor data telah melibatkan pengekspor data untuk menyediakan layanan online tertentu seperti yang dijelaskan dalam Perjanjian.

Kategori data

Data pribadi yang ditransfer menyangkut kategori data berikut (harap tentukan):

Konten yang diunggah oleh Pengekspor Data, atau sebagaimana diberi tahu oleh Pengekspor Data kepada Pengimpor Data dari waktu ke waktu.

Kategori khusus data

Data pribadi yang ditransfer menyangkut kategori khusus data berikut (harap tentukan):

Konten yang diunggah oleh Pengekspor Data, atau sebagaimana diberi tahu oleh Pengekspor Data kepada Pengimpor Data dari waktu ke waktu.

Operasi pemrosesan

Data pribadi yang ditransfer akan tunduk pada kegiatan pemrosesan dasar berikut (harap tentukan): Pengimpor Data akan memproses data pribadi untuk mendukung kegiatan yang dilakukan oleh Pengekspor Data. Secara khusus, kegiatan pemrosesan Pengimpor Data yang dilakukan berdasarkan instruksi dan atas nama Pengekspor Data meliputi: hosting data, pencadangan data, komunikasi, analitik data, statistik, analisis, administrasi sistem TI, pemenuhan pesanan, layanan dukungan, layanan manajemen karyawan, pembayaran pesanan pemrosesan, pengiriman komunikasi pemasaran, promosi dan survei, operasi, pemeliharaan dan hosting perangkat lunak, layanan teknologi informasi termasuk desktop dan manajemen jaringan, pemantauan sistem, pengembangan aplikasi dan program, pengarsipan, manajemen bencana, dan pemulihan data.

Lampiran 2

Langkah-langkah Keamanan Teknis dan Organisasi

Kami telah menerapkan program privasi dan keamanan yang komprehensif untuk tujuan melindungi konten Anda. Program ini mencakup hal-hal berikut:

1. **Keamanan data.** Kami telah merancang dan menerapkan langkah-langkah berikut untuk melindungi data pelanggan terhadap akses yang tidak sah:

   a. standar untuk kategorisasi dan klasifikasi data;
   b. satu set kemampuan autentikasi dan kontrol akses pada tingkat fisik, jaringan, sistem dan aplikasi; dan
   c. mekanisme untuk mendeteksi perilaku abnormal berbasis data besar.
2. **Keamanan jaringan.** Kami menerapkan aturan ketat tentang isolasi jaringan internal untuk mencapai kontrol akses dan perlindungan perbatasan untuk jaringan internal (termasuk jaringan kantor, jaringan pengembangan, jaringan pengujian, dan jaringan produksi) melalui isolasi fisik dan logis.
3. **Keamanan fisik dan lingkungan.** Kontrol akses infrastruktur dan lingkungan yang ketat telah diterapkan untuk pusat data Tencent Cloud berdasarkan persyaratan keamanan regional yang relevan. Matriks kontrol akses didirikan, berdasarkan jenis personel pusat data dan hak akses masing-masing, untuk memastikan manajemen dan kontrol akses dan operasi yang efektif oleh personel pusat data.
4. **Manajemen insiden.** Kami mengoperasikan pemantauan layanan aktif dan real-time, dikombinasikan dengan mekanisme respons dan penanganan yang cepat, yang memungkinkan deteksi dan penanganan insiden keamanan yang segera.
5. **Kepatuhan terhadap standar.** Kami mematuhi standar yang tercantum di halaman Pusat Kepatuhan kami, dan sebagaimana diperbarui dari waktu ke waktu.