PayPal

>> Visa alla juridiska avtal

Företagsbestämmelser för PayPal-användare

PayPal-koncernens mål är att tillämpa enhetliga, lämpliga och globala dataskydds- och integritetsstandarder för hantering av alla personuppgifter som tillhör användare, inom hela PayPal-koncernen. Dessa företagsbestämmelser för användare är tillämpbara för alla personuppgifter som tillhör användare och som behandlas av koncernföretag över hela världen.

Användarna tillhandahåller sina personuppgifter globalt till koncernföretagen för att utnyttja de tjänster som koncernen erbjuder. De flesta personuppgifter som tillhör användare samlas in och lagras i USA. PayPals globala verksamhet kräver att användarpersonuppgifter delas med andra PayPal-enheter i USA och globalt där PayPal för närvarande har eller avser att ha närvaro.

För närvarande kan anställda i följande EES-länder ha tillgång till användarnas personuppgifter: Luxemburg, Belgien, Frankrike, Tyskland, Irland, Italien, Nederländerna, Polen, Spanien och Sverige.

Anställda som för närvarande befinner sig i följande länder utanför EU kan också ha tillgång till användarnas personuppgifter: USA, Taiwan, Turkiet, Jungfruöarna (brittiska), Australien, Kanada, Kina, Hongkong, Indien, Indonesien, Israel, Japan, Sydkorea, Malaysia, Mauritius, Filippinerna, Ryssland, Singapore, Schweiz, Storbritannien Argentina, Brasilien och Mexiko.

PayPal har åtagit sig att skydda användarnas uppgifter på ett lämpligt sätt, oavsett var personuppgifterna lagras, och att tillhandahålla ett lämpligt skydd för användarnas personuppgifter om dessa överförs utanför EES-området.

Denna lista över länder kan komma att ändras när företagets verksamhet växer.

1. Ledningsstruktur vad gäller sekretess samt ansvarsområden

Företagsbestämmelserna för användare är juridiskt bindande enligt ett avtal ("IGA-avtalet") som ingåtts mellan PayPal (Europa) S.à r.l. & Cie, S.C.A ("huvudsakligt koncernföretag") och andra koncernenheter inom PayPal. Enligt IGA-avtalet måste samtliga koncernföretag följa dessa företagsbestämmelser för användare.

Koncernföretagen är skyldiga att se till att de anställda följer dessa företagsbestämmelser för användare när de hanterar användarnas personuppgifter.

Företagsledare och ledande befattningshavare inom PayPal-koncernen ansvarar för att dessa företagsbestämmelser för användare efterlevs. Detta innebär också att de är skyldiga att se till att de anställda känner till och följer dessa företagsbestämmelser för användare.

Det är chefen för efterlevnad av sekretessreglerna som är ansvarig för PayPals integritetsprogram. Han eller hon innehar en högre befattning inom PayPal Holdings, Inc. och rapporterar direkt till den huvudansvarige för regelefterlevnad, eller till den högsta chef som leder arbetet med regelefterlevnad på PayPal. Chefen för efterlevnad av sekretessreglerna övervakar Paypals globala team för integritetsskydd och regelefterlevnad och interagerar med andra interna organisationer eller arbetsgrupper – till exempel drift, IT-säkerhet, regelefterlevnad, riskhantering samt internrevision – för att hjälpa till att säkerställa konsekventa kommunikationer, metoder och riktlinjer gällande sekretess inom hela PayPal-koncernen och på global nivå. Paypals globala team för integritetsskydd och regelefterlevnad utvecklar och samordnar implementeringen av dess efterlevnadsstrategi inom hela PayPal-koncernen och kontrollerar att den följs i den dagliga verksamheten. Paypals globala team för integritetsskydd och regelefterlevnad har direkta eller indirekta representanter inom PayPal-koncernen som, bland annat, hjälper till att säkerställa att företagsbestämmelserna för användare samt gällande dataskyddslagar följs.

Chefen för juridiskt sekretesskydd övervakar PayPals globala rättsliga team för integritetsskydd och rapporterar direkt till chefsjuristen eller högsta chef som ansvarar för de juridiska funktionerna på PayPal. Chefen för juridiskt sekretesskydd definierar koncernens skyldigheter enligt gällande dataskyddslagar och dessa företagsbestämmelser för användare. Chefen för juridiskt sekretesskydd och PayPals globala juridiska team för integritetsskydd har ett nära samarbete med chefen för efterlevnad av sekretessreglerna samt med Paypals globala team för integritetsskydd och regelefterlevnad. De samarbetar också med andra interna organisationer och arbetsgrupper – till exempel den rättsliga avdelningen, drift, IT-säkerhet och riskhantering – för att tillhandahålla juridisk rådgivning och förklara juridiska och rättsliga konsekvenser vid pågående integritetsärenden inom den globala PayPal-koncernen.

Paypals globala team för integritetsskydd och regelefterlevnad och PayPals globala juridiska team för integritetsskydd kommer hädanefter att kallas för "PayPals globala styrgrupp för sekretessarbete", som ett samlingsnamn för båda dessa avdelningar.

Det europeiska dataskyddsombudet (DPO) i Luxemburg utnämns av och rapporterar till ledningen för PayPal (Europa) S.à r.l. et Cie, S.C.A. Det europeiska dataskyddsombudet fungerar som den huvudsakliga kontaktpersonen för dataskyddsmyndigheterna inom EES-området och har bland annat följande arbetsuppgifter: informera och ge råd till koncernföretagen och de anställda som behandlar personuppgifter vad gäller deras skyldigheter enligt sekretesslagstiftningen för att säkerställa efterlevnaden av dessa

företagsbestämmelser för användare; arbeta med PayPals globala styrgrupp för sekretessarbete för att övervaka efterlevnaden av sekretesslagstiftningen och relaterade riktlinjer för koncernföretagen och tillhandahålla juridisk rådgivning till koncernföretagen, på begäran av dessa, om dataskyddets påverkan och implementeringen av dataskydd.

2. Principer för behandling av personuppgifter som tillhör användare

Koncernföretagen efterlever följande behandlingsprinciper vad gäller personuppgifter som tillhör användare.

2.1 Ändamålsbegränsning

Användarnas personuppgifter får endast behandlas för specifika, explicita och legitima ändamål. I synnerhet kan användarnas personuppgifter behandlas för att

– erbjuda och underlätta tillhandahållandet av tjänster på användarnas begäran, inklusive öppnandet av ett konto

– förbättra tjänsterna och utveckla nya tjänster

– lösa tvister, hantera rättstvister, felsöka problem och tillhandahålla kundservice

- utföra riskhantering

– behandla transaktioner och driva in fordringar

– kontrollera kreditvärdighet och betalningsförmåga

– utvärdera användarnas intresse för tjänster samt deras feedback och synpunkter och informera användare om erbjudanden, både online och offline, samt om tjänster och uppdateringar

– anpassa användarupplevelsen

– upptäcka och förebygga fel, bedrägerier och annan brottslig verksamhet

– uppfylla PayPal-koncernens juridiska, avtalsenliga eller lagstadgade skyldigheter

– se till att villkoren för tjänsten efterlevs och samt de andra regler som beskrivs för användarna vid tidpunkten för insamling av uppgifter och de bestämmelser som återfinns i sekretesspolicyn för tjänsten

– skydda tjänsternas säkerhet, integritet och tillgänglighet samt PayPal-koncernens nätverk

– skydda PayPal-koncernens lagstadgade rättigheter och intressen inklusive, men inte begränsat till, att fastställa, utöva eller försvara sig mot rättsliga anspråk.

Behandlingen av personuppgifter som tillhör användare för andra ändamål är föremål för förhandsgodkännande av PayPals globala juridiska team för integritetsskydd. Vid tveksamheter ska koncernföretagen rådfråga PayPals globala juridiska team för integritetsskydd.

Användarnas personuppgifter ska inte behandlas ytterligare på ett sätt som är oförenligt med de ovan angivna ändamålen, såvida det inte finns en rättslig grund för det koncernföretag inom EES-området som är ansvarigt för insamlingen och/eller överföringen av användarnas personuppgifter att göra detta i enlighet med tillämplig lag.

2.2 Datakvalitet och -proportionalitet

Personuppgifter som tillhör användare ska vara

- korrekta och, om så krävs, uppdaterade
- lämpliga, relevanta och inte överdrivna i förhållande till de syften som de behandlas för
- inte lagras längre än vad som krävs för att uppnå de ändamål för vilka de ursprungligen samlades in eller vidarebehandlades.

De personuppgifter som tillhör användare som man inte längre behöver lagra för de ändamål för vilka de ursprungligen behandlades, ska tas bort, raderas, förstöras eller anonymiseras, såvida det inte finns rättslig grund för vidare behandling eller om lagring krävs enligt gällande lag.

2.3 Rättsliga grunder för behandlingen

Koncernföretagen ska se till att användarnas personuppgifter behandlas rättvist och lagligt och i synnerhet på grundval av minst en av följande rättsliga grunder:

- Otvetydigt medgivande från användarens sida
- Behandling som är nödvändig för att fullgöra ett avtal i vilket användaren är part eller för att vidta åtgärder på begäran av användaren innan ett sådant avtal ingås
- Behandling som är nödvändig för att uppfylla de rättsliga förpliktelser som koncernföretagen är underställda
- Behandling som är nödvändig för att skydda användarens väsentliga intressen
- Behandling som är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning av koncernföretagen eller en tredje man till vilken uppgifterna har lämnats ut

- Behandling som är nödvändig för ändamål som rör koncernföretagets berättigade intressen, eller en tredje man till vilken uppgifterna har lämnats ut, utom när sådana intressen uppvägs av användarens intressen eller dennas grundläggande fri- och rättigheter.

Som grundregel samlar koncernföretagen inte in känsliga personuppgifter från användarna. Om sådan insamling krävs, eller användare frivilligt tillhandahåller sådan information, ska koncernföretagen se till att de känsliga personuppgifter som tillhör användarna enbart behandlas på basis av minst en av följande grunder:

- Uttryckligt medgivande från användarens sida
- Behandling som är nödvändig för att skydda intressen som är väsentliga för användaren eller någon annan person om användaren är fysiskt eller rättsligt oförmögen att ge sitt samtycke
- Behandlingen rör personuppgifter tillhörande användare som på ett tydligt sätt har offentliggjorts av användaren själv
- Behandling som är nödvändig för att kunna fastslå, göra gällande eller försvara rättsliga anspråk.

Om behandlingen innefattar automatiskt beslutsfattande ("automatiska beslut") ska koncernföretagen tillhandahålla lämpliga åtgärder för att skydda användarens legitima intressen, till exempel ge användaren möjlighet att få tillgång till en kundtjänstrepresentant som kan granska det enskilda beslutet och låta användaren ange sin ståndpunkt. Kundtjänstrepresentanten ska eskalera ärendet till EU:s dataskyddsombud om användaren fortsätter att bestrida ett automatiserat beslut. Om tillämpligt kommer chefen för juridiskt sekretesskydd att konsulteras och chefen för efterlevnad av sekretessregler att underrättas.

2.4 Transparens

Vid insamlingen av användarnas personuppgifter ska koncernföretagen informera användarna om följande:

- Namnet på och adressen till det koncernföretag som är ansvarigt för den ursprungliga insamlingen och behandlingen
- Vilka kategorier av personuppgifter det handlar om
- Avsett ändamål med behandlingen
- Kategorier av personuppgiftsbiträden och tredje parter som tar emot användarnas personuppgifter
- Om svar på frågorna är obligatoriska eller frivilliga, samt de möjliga följderna om svar inte ges
- Om det finns några användarrättigheter
- Vilken logik som är involverad om automatiserat beslutsfattande används.

Koncernföretagen kan tillhandahålla informationen i sekretesspolicyn för en tjänst. Denna ska vara tillgänglig via en länk och/eller visas på en framträdande plats på varje

webbplats eller program för tjänsten samt under registreringen. Skyldigheten att informera användaren gäller inte om användaren redan känner till informationen.

Om det inte är möjligt att tillhandahålla informationen eller om det skulle innebära en oproportionerligt stor ansträngning, kan koncernföretagen avstå från att tillhandahålla informationen. Detta skulle enbart gälla personuppgifter som inte har erhållits direkt från användaren.

I undantagsfall kan tillhandahållandet av specifik information skjutas upp eller utelämnas, till exempel i samband med utredningar om tjänstefel eller för att följa gällande lagar eller där det skulle äventyra utredningens integritet att tillhandahålla informationen.

2.5 Sekretess och säkerhet

Koncernmedlemmarna vidtar fysiska, tekniska och organisatoriska säkerhetsåtgärder som står i proportion till antalet personuppgifter samt hur känsliga dessa är. Detta för att förhindra obehörig behandling, inklusive men inte begränsat till, obehörig åtkomst till, förvärv och användning av, förlust av, skador på eller förstörelse av personuppgifter som tillhör användare. Koncernföretagen använder kryptering, brandväggar, åtkomstkontroller, standarder och andra förfaranden för att skydda användarinformation från obehörig åtkomst. Fysisk och logisk åtkomst till elektroniska dokument och papperskopior är ytterligare begränsad baserat på vilka ansvarsområden personen i fråga har samt på verksamhetsbehoven.

2.6 Användarval och användarrättigheter

Användarna kan få tillgång till och korrigera huvuddelen av de personuppgifter som rör dem och som koncernföretagen lagrar. Dessa rättigheter kan hävdas genom att ett lämpligt verktyg på nätet eller självbetjäningsprocesser som görs tillgängliga via tjänstens webbplats eller program används.

Användarna har alltid rätt att begära dataåtkomst för att se eller få en kopia av registrerade personuppgifter som inte är tillgängliga via tjänstens webbplats eller program. Användarna bör kontakta kundtjänst med hjälp av de anvisningar som tillhandahålls via tjänstens webbplats eller program. Koncernföretagen ska behandla förfrågningar inom de tidsramar som föreskrivs av tillämplig lag, förutom då tillämplig lag innehåller undantag vad gäller denna skyldighet. Användarna kan behöva styrka sin identitet och kan komma att debiteras en serviceavgift. Denna avgift regleras enligt tillämplig lag.

Användare kan även begära rättelse av sina uppgifter om de är ofullständiga eller felaktiga. Koncernföretagen ska uppfylla kraven i en sådan begäran och informera användare om när deras uppgifter har korrigerats. Koncernföretagen kommer att meddela alla tredje parter till vilka användarens data har vidarebefordrats om alla rättelser som görs, såvida inte detta är omöjligt eller innebär en oproportionerligt stor ansträngning.

Vid avgörande och berättigade skäl kan användare göra invändningar mot behandlingen av sina personuppgifter. Koncernföretagen ska följa kraven i sådana förfrågningar, såvida inte lagring av användarnas personuppgifter krävs enligt gällande lag eller för att försvara PayPal-koncernens intressen vid rättsliga anspråk. Användarna kommer att informeras om resultatet av deras begäran och vilka åtgärder som vidtagits av koncernföretagen.

Användarna kan dessutom begära att deras konton ska stängas, genom att följa anvisningarna som tillhandahålls via tjänstens webbplats eller program. Koncernföretagen ska ta bort eller anonymisera en användares uppgifter från en tjänst så fort som möjligt baserat på kontoaktiviteten. Koncernföretagen kan fördröja nedstängningen av ett konto eller behålla användarnas personuppgifter för att utföra en undersökning eller då det krävs enligt tillämplig lag. Koncernföretagen kan också behålla användaruppgifter från stängda konton för att upptäcka och förebygga bedrägerier, debitera avgifter, lösa tvister, felsöka problem, underlätta utredningar, utföra riskhantering, genomdriva tjänstevillkor, efterleva rättsliga och lagstadgade krav samt för att vidta andra åtgärder som är tillåtna enligt tillämplig lag. Uppgifterna kommer att lagras i en form som tillåter identifiering av de registrerade, men inte under längre tid än vad som är nödvändigt för det ändamål för vilket dessa data samlades in eller för vilket de vidarebehandlas. De kommer att raderas så fort den underliggande orsaken till lagringen är uppklarad eller löst.

Med undantag för de användare som har valt att inte ta emot viss kommunikation kan koncernföretagen använda användarnas personuppgifter för att skicka riktad kommunikation till användarna utifrån deras intressen enligt gällande lag. Användare som inte vill få marknadsföringsmaterial från PayPal-koncernen kommer att erbjudas en lättillgänglig metod för att invända mot vidare reklam, till exempel i kontoinställningarna eller genom att följa anvisningar givna i e-postmeddelanden eller via en länk i kommunikationen.

Användare kan utöva ovanstående rättigheter genom att kontakta kundtjänst. Om en användares identitet är svår att verifiera kan koncernföretagen kräva att användaren stärker sin identitet genom att skicka in ytterligare identifieringsbevis.

2.7 Överföring av personuppgifter

Koncernföretagen kan dela personuppgifter som tillhör användare inom ramen för organisationens bedrivande av den dagliga verksamheten med andra koncernföretag över hela världen. Dessa överföringar kan göras för de ändamål som anges i avsnitt 2.1.

I enlighet med gällande lag, avtal eller tillämpliga internationella konventioner kan koncernföretagen dela personuppgifter med polismyndigheter och tillsynsmyndigheter när det krävs i ett demokratiskt samhälle för att skydda nationell säkerhet, skydda rikets säkerhet, trygga den allmänna säkerheten; för att förebygga, utreda, identifiera brott och väcka åtal; och, i synnerhet följa sanktioner som fastställs via internationella och/eller nationell instrument, skattedeklarationskrav eller rapporteringskrav gällande bekämpning av penningtvätt.

Koncernföretagen varken säljer eller hyr ut användarnas personuppgifter till tredje parter för egna marknadsföringsändamål utan användarens uttryckliga och entydiga informerade samtycke. Koncernföretagen kan överföra användarinformation till andra tredje parter i enlighet med användarens anvisningar eller samtycke (om det är tillåtet enligt gällande lag).

Vid överföring av användaruppgifter till personuppgiftsbiträden kommer dessa personuppgiftsbiträden att bli föremål för riskbedömning gällande personuppgifter, dataskydd och informationssäkerhet innan arbetet inleds och innan överföringen av användaruppgifterna sker. Omfattningen av bedömningen kommer att variera baserat på hur känsliga de behandlade användaruppgifterna är. Personuppgiftsbiträdena, inklusive koncernföretag som agerar som ett personuppgiftsbiträde, måste ingå ett avtal med de relevanta koncernföretagen för att tillhandahålla lämpliga åtgärder för integritet, dataskydd och informationssäkerhet. Ett sådant avtal ska inkludera klausuler som säkerställer lämplig användning av användaruppgifterna och säkerhetsåtgärder som står i proportion till personuppgifternas antal, beskaffenhet och känslighet. Som minimum ska avtalsgarantierna omfatta följande:

- Skyldighet att följa gällande lagar och krav om att behandla användarnas personuppgifter i enlighet med villkoren i avtalet samt enbart enligt anvisningar som ges av de berörda koncernföretagen.
- Lämpliga tekniska och organisatoriska åtgärder anpassade efter personuppgifternas känslighet och den behandling som är involverad.
- Rätten att kontrollera om personuppgiftsbiträdet efterlever avtalsgarantierna.
- Skyldighet att avisera vid brott mot säkerheten.
- Bestämmelser om korrigerande åtgärder från personuppgiftsbiträdets sida i händelse av brott mot rättsliga skyldigheter eller avtalsförpliktelser.

Avtalen ska innehålla bestämmelser som säkerställer att underlåtenhet att följa avtalsvillkoren kan leda till uppsägning av avtalet, bland andra korrigerande åtgärder som anges i avtalet.

Bedömningen gällande sekretess, dataskydd och informationssäkerhet är inte obligatorisk för personuppgiftsbiträden som redan har genomgått en sådan bedömning, såvida inte databehandlingsaktiviteterna inbegriper högriskaktiviteter. I dessa ärenden ska man ta hänsyn till antalet personuppgifter och deras beskaffenhet samt vilka typer av databehandlingsaktiviteter som är involverade.

Oavsett vad som nämns ovan, ska koncernföretagen – när de överför personuppgifter från användare som är bosatta i EES-området till tredje parter eller personuppgiftsbiträden som inte är koncernföretag: (i) som har sitt säte i länder som inte tillhandahåller adekvata skyddsnivåer (enligt definitionen i direktivet 95/46/EG),) (ii) som inte omfattas av godkända och bindande verksamhetsregler, eller (iii) som inte har inrättat andra åtgärder som skulle uppfylla EU:s lämplighetskrav – ge följande försäkringar:

- Tredje parter: Att de ska införa lämpliga avtalskontroller, till exempel enligt den modell för avtalsvillkor som godkänts av Europeiska kommissionen, och att tillhandahålla skyddsnivåer motsvarande dessa företagsbestämmelser för användare eller, alternativt, se till att överföringen (i) äger rum med ett tydligt medgivande från användarens sida, (ii) är nödvändig för att avsluta eller utföra ett avtal som ingåtts med användaren, (iii) är nödvändig eller ett lagstadgat krav med viktiga allmänintressen eller (iv) är nödvändig för att skydda användarens väsentliga intressen
- Personuppgiftsbiträden: Att de ska införa avtalskontroller, till exempel enligt den modell för avtalsvillkor som godkänts av Europeiska kommissionen, och att tillhandahålla skyddsnivåer motsvarande dessa företagsbestämmelser för användare.

3. Klagomålsförfarande

Om användarna tror att det begåtts något brott mot företagsbestämmelserna för användare vid behandlingen av deras personuppgifter, kan de rapportera problemet till kundtjänstavdelningen hos koncernföretaget i fråga. Detta kan göras via webbplatsen som är kopplad till den relevanta tjänsten, e-post eller annat sätt som anges i tillämpliga villkor. Användarna kan i allmänhet hitta svar på de vanligaste sekretessfrågorna och -problemen genom att skriva in ordet "sekretess" (eller "privacy") i hjälpavsnittet för tjänsten i fråga. Då dirigeras normalt användaren vidare till en specifik sida eller policy om sekretess. Avsnittet "Hjälp" (Help) för den relevanta tjänsten är en unik portal för alla användarfrågor gällande till integritet eller behandling av användarinformation. Här har användarna även möjlighet att kontakta kundtjänst.

Om det råder tvekan om vilken kanal som ska användas för att rapportera sekretessrelaterade problem kan användarna kontakta det europeiska dataskyddsombudet via internet.

Kundtjänsten undersöker och försöker att lösa problem som tagits upp av användare. Anställda som är ansvariga för hantering av integritetsrelaterade frågor arbetar med PayPals globala styrgrupp för sekretessarbete och ger användarna svar i enlighet med PayPals riktlinjer, procedurer och vägledning. Om användarna tycker att deras ärende inte har behandlats på rätt sätt, eller om de inte har fått svar, kan de begära att deras ärende förs vidare och eskaleras till det europeiska dataskyddsombudet. Chefen för juridiskt sekretesskydd kommer att rådfrågas och chefen för efterlevnad av sekretessreglerna att underrättas. Vilka vägar för eskalering som ska användas bestäms utifrån ärendets beskaffenhet och omfattning och ärendet ska vidarebefordras till lämplig arbetsgrupp utan fördröjning. Ett svar på klagomålet ska ges till användaren inom en rimlig tidsperiod, och i samtliga fall senast tre (3) månader efter datumet då klagomålet skickades in. Detta gäller i samtliga fall, utom vid ovanliga omständigheter eller komplicerade frågor, då användaren informeras om att det kommer att ta längre än tre (3) månader att lösa ärendet.

Mekanismen för klagomålshantering påverkar inte användarnas rätt att föra vidare klagomålet till behöriga dataskyddsmyndigheter eller till en domstol.

4. Tredje parts förmånsrättigheter och skadeståndsansvar

Användare inom EES-området som misstänker brott mot företagsbestämmelserna för användare utanför EES, har rätt att kräva att företagsbestämmelserna för användare ska tillämpas som tredjepartsberättigande för avsnitt 2, 3, 4, 7 och 8 i företagsbestämmelserna för användare inför behöriga dataskyddsmyndigheter, inför domstolar i relationer med det huvudsakliga koncernföretaget eller inför domstolar i relationer med koncernföretag som fungerar som dataexportör. Dessa rättigheter till upprätthållande kan utnyttjas tillsammans med andra avhjälpande åtgärder eller rättigheter som tillhandahålls av PayPal eller som är tillgängliga enligt tillämplig lag.

Även om det inte är obligatoriskt uppmuntras användare inom EES-området att först rapportera sitt problem direkt till koncernföretaget snarare än till dataskyddsmyndigheterna eller en domstol. Detta möjliggör ett effektivt och snabbt svar från PayPal-koncernens sida och minimerar eventuella förseningar som kan uppstå om man går direkt till dataskyddsmyndigheterna eller via ett domstolsförfarande.

PayPal Europe S.à r.l. et Cie, S.C.A., ett privat aktiebolag med säte i Luxemburg, ansvarar för och samtycker till att övervaka koncernföretagets efterlevnad av företagsbestämmelserna för användare. Det huvudsakliga koncernföretaget åtar sig (i) att vidta nödvändiga åtgärder för att avhjälpa ett brott som begåtts av koncernföretag utanför EES-området; och (ii) att betala ersättning till EES-användare som tilldömts av den ledande datatillsynsmyndigheten eller en domstol i Luxemburg för eventuella skador som direkt beror på ett brott mot företagsbestämmelserna för användare av ett koncernföretag utanför EES, om det berörda koncernföretaget inte kan eller vill betala ersättningen eller följa ordern.

Det huvudsakliga koncernföretaget erkänner och accepterar att det bär bevisbördan vad gäller påstådda överträdelser av företagsbestämmelserna för användare.

Det huvudsakliga koncernföretaget (eller något annat koncernföretag) kan inte hållas ansvarigt om det rimligen kan bevisa, på grundval av de tillgängliga uppgifterna och genom att ta hänsyn till användarens kommentarer, att koncernföretaget som befinner sig utanför EES inte har brutit mot företagsbestämmelserna för användare eller inte har orsakat de skador som användaren hävdar.

5. Utbildning

Koncernföretagen kommer att se till att alla anställda som behandlar personuppgifter som tillhör användare samt de anställda som är involverade i utformandet av verktyg som ska användas för att samla in eller behandla personuppgifter, genomgår lämplig utbildning för att öka medvetenheten om sekretess och informationssäkerhet. Detta för att betona vikten av dessa aspekter och informera de anställda om behovet av att skydda användarnas personuppgifter i enlighet med dessa företagsbestämmelser för användare.

Anställda är varje år skyldiga att genomgå en onlineutbildning i regelefterlevnad. Denna utbildning fokuserar på koncernens uppförandekod samt etik och innehåller ett avsnitt om dataskydd. Nyanställda ska genomgå onlineutbildningen i regelefterlevnad när de inleder sin anställning på koncernen.

Utöver denna onlineutbildning i regelefterlevnad håller PayPals globala styrgrupp för sekretessarbete och det europeiska dataskyddsombudet kurser för att öka medvetenheten om sekretess och informationssäkerhet. Detta för att betona vikten av dessa aspekter och informera de anställda om behovet av att skydda personuppgifter. Sådan utbildning genomförs på årsbasis eller oftare om omständigheter kräver det.

Den utbildning som de anställda får ska anpassas efter deras behörighet vad gäller åtkomst till användarnas personuppgifter. Ytterligare utbildning ska erbjudas anställda med större behörighet och högre åtkomstnivåer.

Koncernföretagen ska informera anställda om att underlåtenhet att följa dessa företagsbestämmelser för användare kan leda till disciplinära åtgärder och andra åtgärder som är tillåtna enligt gällande lag. En kopia av dessa företagsbestämmelser för användare och andra relevanta riktlinjer och procedurer gällande sekretess och informationssäkerhet finns tillgängliga för alla anställda, när som helst, via företagets intranät. Företagsbestämmelser för användare finns även inkluderade i Koden för uppförande och etik som alla anställda måste läsa och samtycka till att följa.

6. Revisioner och övervakning

För att säkerställa efterlevnaden av dessa företagsbestämmelser för användare övervakar PayPals globala team för integritetsskydd och regelefterlevnad kontinuerligt aktiviteter som är kopplade till behandlingen och hanteringen av personuppgifter. Denna övervakning koordineras i samråd med det europeiska dataskyddsombudet.

Internrevisionsgruppen är en oberoende och objektiv rådgivare till ledningen och styrelsen, som kommunicerar resultatet av revisionerna, via revisionsutskottet, till styrelsen, chefer som har ansvar för sekretessarbete och till det europeiska dataskyddsombudet.

Internrevisionsgruppen kan regelbundet göra en översyn av aktiviteter eller metoder som har identifieras av den globala styrgruppen för sekretessarbete. Internrevisionsgruppen,

chefer med ansvar för sekretessarbete och det europeiska dataskyddsombudet ska, om så är nödvändigt, kräva att en åtgärdsplan tas fram för att säkerställa efterlevnad av de bindande företagsbestämmelserna (BCR). Om de interna arbetsgrupperna inte kan lösa ett ärende på ett tillfredsställande sätt, kan koncernen utse oberoende, externa revisorer att lösa problemet.

Det europeiska dataskyddsombudet, PayPals globala styrgrupp för sekretessarbete – eller internrevisionsgrupperna och externa revisorer – tar fram utförliga revisionsplaner och -program baserat på den risk som är kopplad till behandlingen.

Resultatet av sekretessrevisionerna kommer att vara tillgängligt för behöriga tillsynsmyndigheter för dataskydd (DPA). PayPal förbehåller sig rätten att redigera delar av revisionsrapporterna för att se till att ingen information om immateriella rättigheter eller annan konfidentiell företagsinformation röjs.

7. Förhållandet mellan företagsbestämmelserna för användare och nationell lagstiftning

De lagstadgade kraven gällande dataskydd varierar stort i olika delar av världen. Företagsbestämmelserna för användare är en konsekvent uppsättning av krav för att säkerställa en lämplig behandling av personuppgifter som tillhör användare. Men även om företagsbestämmelserna för användare utgör en god bas för de grundläggande krav som koncernföretagen måste rätta sig efter, kommer koncernföretagen också att följa tillämpliga lagar som kan införa strängare regler än de som anges i dessa företagsbestämmelser för användare.

Ingenting i dessa företagsbestämmelser för användare påverkar ett koncernföretags skyldigheter enligt gällande lagar om bankverksamhet, särskilt vad gäller banksekretessen. Om tillämpliga lagar strider mot dessa företagsbestämmelser för användare i det avseende att det skulle kunna förhindra ett koncernföretag från att fullfölja sina skyldigheter enligt dessa företagsbestämmelser för användare och att det har en stor effekt på garantierna givna däri, ska koncernföretaget omedelbart informera det europeiska dataskyddsombudet, utom då tillhandahållandet av sådan information är förbjuden enligt en brottsbekämpande myndighet eller enligt lag. Det europeiska dataskyddsombudet, cheferna för sekretessfrågor och det huvudsakliga koncernföretaget ska fastställa en lämplig åtgärdsplan och, om det råder tveksamhet, rådgöra med behörig dataskyddsmyndighet.

8. Ömsesidig rättslig hjälp och samarbete med dataskyddsmyndigheter

Koncernföretagen kommer att samarbeta och hjälpa varandra för att hantera frågor eller klagomål från användare som är kopplade till dessa företagsbestämmelser för användare.

Koncernföretagen kommer att besvara förfrågningar från dataskyddsmyndigheter gällande företagsbestämmelserna för användare på ett lämpligt sätt och inom rimlig tid. Om en anställd tar emot en sådan begäran från en dataskyddsmyndighet bör han/hon omedelbart informera det europeiska dataskyddsombudet.

Koncernföretagen kommer att vara samarbetsvilliga vid förfrågningar och godta revisioner från behöriga dataskyddsmyndigheter inom EES vad gäller efterlevnad med dessa företagsbestämmelser för användare. Företagen kommer att respektera beslut som tas i enlighet med gällande lag och rättsliga förfaranden.

9. Uppdateringar av innehållet i dessa företagsbestämmelser för användare och lista över förpliktigade koncernföretag

PayPal förbehåller sig rätten att ändra dessa företagsbestämmelser för användare efter behov, till exempel, för att anpassa dem efter ändringar i tillämplig lag, regler, bestämmelser samt PayPals praxis, procedurer och organisatoriska struktur eller krav som ställs av relevanta dataskyddsmyndigheter.

PayPals globala, juridiska team för integritetsskydd (under ledning av chefen för juridiskt sekretesskydd), kommer att föreslå eventuella ändringar som behöver göras i dessa företagsbestämmelser för användare. PayPals globala styrgrupp för sekretessarbete (under ledning av chefen för efterlevnad av sekretessreglerna) och det europeiska dataskyddsombudet, måste godkänna alla ändringar i företagsbestämmelserna för användare och ska spåra alla ändringar av företagsbestämmelserna för användare samt eventuella ändringar i listan över koncernföretag. Koncernföretagen ska rapportera eventuella ändringar i företagsbestämmelserna för användare till de relevanta dataskyddsmyndigheterna för formellt godkännande och enligt de krav som ställs i gällande lag.

Det huvudsakliga koncernföretaget kommer att samråda med den ledande dataskyddsmyndigheten om väsentliga ändringar av användarföretagets regler som skulle påverka efterlevnaden av dataskyddet eller användningen av företagsbestämmelserna för användare. Det huvudsakliga koncernföretaget kommer att kommunicera större ändringar i företagsbestämmelserna för användare och ändringar i listan över koncernföretag minst en gång om året till den ledande dataskyddsmyndigheten. PayPals globala styrgrupp för sekretessarbete kommer att samarbeta för att ge stöd till det europeiska dataskyddsombudet. Denna enhet kommer i synnerhet att samordna åtgärder och snabbt ta uti med kommentarer, förslag eller invändningar gällande ändringarna som har lagts fram av den ledande dataskyddsmyndigheten å PayPals vägnar. Alla kommentarer, förslag eller invändningar som tas upp av andra dataskyddsmyndigheter kommer att kommuniceras till det europeiska dataskyddsombudet via den ledande dataskyddsmyndigheten. Den senare ska agera på andra dataskyddsmyndigheters vägnar.

Ändringar i företagsbestämmelserna för användare ska gälla för samtliga koncernföretag från och med det angivna införingsdatumet. Koncernföretagen kommer att skicka ut meddelanden om större förändringar i företagsbestämmelserna för användare i enlighet med användarens inställningar för tjänsten. Detta kommer antingen att göras genom ett massutskick via e-post eller ett inlägg på webbplatsen. Användarna kommer därmed i god tid att få en varning om att bestämmelserna har ändrats. Koncernföretagen ska lägga ut de reviderade företagsbestämmelserna för användare på utvalda externa webbplatser eller i program som användarna har tillgång till. Revideringar av företagsbestämmelser för användare kommer att börja gälla inom två månader efter att koncernföretaget har informerat användarna och skickat eller lagt ut de reviderade företagsbestämmelser för användare.

10. Publicering

Företagsbestämmelserna för användare ska publiceras och en länk ska göras tillgänglig på tjänstens webbplats eller i dess program. Användare kan begära en kopia från det europeiska dataskyddsombudet på: The European Data Protection Officer (DPO), PayPal (Europe) S.à r.l et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxemburg eller online.

11. Slutbestämmelser

Giltighetsdatum: 25 maj 2018

Kontaktperson: Om användarna har frågor eller undrar över något vad gäller dessa företagsbestämmelser för användare kan de kontakta:

The European Data Protection Officer (DPO)

PayPal (Europe) S.à r.l. et Cie , S.C.A., 22–24 Boulevard Royal, L-2449 Luxemburg

12. Definitioner

Koncernföretagen ska tolka företagsbestämmelserna för användare på ett sätt som stämmer bäst överens med de grundläggande principerna i EU-direktivet 95/46/EG eller direktiv eller förordningar som ersätter detta.

Följande definitioner är de som gäller i dessa företagsbestämmelser för användare:

Styrelsen syftar på styrelsen för det huvudsakliga koncernföretaget.

Dataskyddsmyndigheter syftar på en offentlig myndighet som ansvarar för övervakningen och efterlevnaden av de nationella dataskyddslagarna inom respektive territorium. De nationella lagarna är de lagar som antagits av EES-medlemsstaterna enligt EU:s dataskyddsdirektiv (95/46/EG).

EES syftar på Europeiska ekonomiska samarbetsområdet som för närvarande består av EU-länderna, Island, Liechtenstein och Norge.

Anställd syftar på anställda, arbetstagare, praktikanter och annan personal eller medarbetare, inklusive tillfälligt anställd personal, alternativ arbetskraft eller ett koncernföretags leverantör, oavsett om personen är anställd eller har anlitats på hel- eller deltid, oavsett typ av anställning eller åtagande.

Europeiska dataskyddsombudet (DPO) syftar på den medarbetare som utses av och rapporterar till ledningen för det huvudsakliga koncernföretaget. Han/hon ingår också i PayPals globala styrgrupp för sekretessarbete. Det europeiska dataskyddsombudet har sitt säte i Luxemburg.

Koncernföretag syftar på en enhet inom PayPal-koncernen som har skrivit under IGA-avtalet.

IGA syftar på det koncerninterna avtalet (Intra-Group Agreement)

Ledande dataskyddsmyndigheten syftar på Commission nationale pour la protection des données ("CNPD") i Luxemburg.

Huvudsakligt koncernföretag syftar på PayPal (Europe) S.à r.l. & Cie, S.C.A., ett privat aktiebolag med säte i Luxemburg.

PayPals globala styrgrupp för sekretessarbete syftar på Paypals globala team för integritetsskydd och regelefterlevnad samt PayPals globala, juridiska team för integritetsskydd, tillsammans.

Paypals globala team för integritetsskydd och regelefterlevnad syftar på medlemmar i organisationen för regelefterlevnad som specifikt hanterar regelefterlevnad och förvaltningen av PayPals integritetsprogram.

PayPals globala, juridiska team för integritetsskydd syftar på medlemmar från den juridiska avdelningen som specifikt hanterar sekretess och dataskydd.

PayPal-koncernen syftar på PayPal Holdings Inc. ("PayPal") och alla andra enheter som kontrolleras direkt eller indirekt av PayPal som behandlar användarinformation. Med "kontrollerar" avses att man äger mer än femtio procent (50 %) av rösträtten för att utse styrelseledamöter till företaget eller över femtio procent (50 %) av ägarandelen i företaget.

Personuppgifter syftar på all information som rör en identifierad eller identifierbar fysisk person. En identifierbar person är en person som kan identifieras, direkt eller indirekt, i synnerhet genom hänvisning till ett ID-nummer eller till en eller flera faktorer som är specifika för hans/hennes fysiska, fysiologiska, mentala, ekonomiska, kulturella eller sociala identitet.

Behandling syftar på en åtgärd eller en uppsättning av åtgärder som involverar personuppgifter, oavsett om detta sker på ett automatiskt sätt, till exempel insamling, registrering, organisation, lagring, anpassning eller ändring, hämtning, konsultation, användning, röjande via överföring, spridning eller annat tillgängliggörande, anpassning eller sammanslagning, blockering, radering eller förstörelse.

Personuppgiftsbiträde syftar på en fysisk eller juridisk person som behandlar personuppgifter på uppdrag av ett koncernföretag.

Känsliga personuppgifter syftar på personuppgifter som avslöjar etnisk bakgrund eller etnisk tillhörighet, politisk, religiös eller filosofisk övertygelse, information gällande förbrytelser eller information som rör hälsa och sexliv.

Tjänst syftar på en webbplats, app, program eller någon annan produkt eller tjänst som tillhandahålls av en enhet inom PayPal-koncernen för användares bruk.

Tredje part syftar på en fysisk eller juridisk person, myndighet, agentur eller något annat organ än användaren, koncernföretaget eller personuppgiftsbiträdet som på direkt order från koncernföretaget eller personuppgiftsbiträdet – till exempel anställda – är behöriga att behandla personuppgifter.

Användare syftar på tidigare och befintliga kunder, potentiella kunder, investerare, företagspartner och handlare.

Användarens personuppgifter, eller personuppgifter som tillhör användare, syftar på personuppgifter som kan kopplas till användare.

.